Code: EHAA-E

EMPLOYEE ACCEPTABLE USE OF TECHNOLOGY

1.0 PURPOSE

1.1 Use of computers and network resources by employees of the District is permitted and encouraged where such use supports the goals and objectives of the District. Communications and computer technology at the District are provided and maintained for instructional, educational and administrative purposes.

1.2 Personal use of communications and computer technology at the District is strictly prohibited during the employee's student contact hours. Personal use is allowable when it does not conflict with the employee's responsibilities and conforms to other District policies, including computer use and student data security policies.

2.0 ACCESS TO TECHNOLOGY EQUIPMENT AND SERVICES

2.1 Access to technology is provided to facilitate the instructional and administrative tasks performed by District employees and volunteers. The level of access provided will coincide with the requirements of each employee's job functions.

2.2 Computer files and communications over electronic networks, including e-mail, voice mail and Internet access, are not exclusively private. It should be understood that through routine maintenance the Technology Department may inadvertently see information. The Technology Department is obligated to maintain confidentiality regarding information about students, employees, or District business that they come in contact with except as directed by the Superintendent or his/her designee. When the administration believes an employee may have engaged in misconduct or as a result of routine monitoring to assure compliance with this policy and the accompanying exhibit, the administration has the right to review computer usage and/or information accessed or stored.

2.3 To ensure proper use, the Technology Department under the direction of the Superintendent/designee may monitor the District's technological resources, including e-mail, voice mail systems and Internet usage, at any time without advance notice or consent.

2.4 School District employees have no expectation of privacy in electronic communications they send or receive on the District's computers or network

system, or as to sites and information accessed utilizing District computers or the networking system. The District has the right to monitor or review any communications sent or received, as well as information regarding sites and/or information accessed.

3.0 ACCEPTABLE USE

3.1 It is a general policy that online communication is to be used in a responsible, efficient, ethical, and legal manner in support of education, school business and/or research and within the educational program and goals of the District. The use of electronic information resources is a privilege, not a right. Each user is personally responsible for this provision at all times when using electronic information services.

3.2 Site administrators, department heads or supervisors may set more restrictive guidelines for employees in their areas of responsibility.

3.3 While electronic information resources offer tremendous opportunities of educational value, they also offer persons with illegal or unethical purposes avenues for reaching students, teachers, and others, including parents. The District does not have control of the information on commercial electronic information services or the information on the Internet, although it attempts to provide prudent and available barriers. Sites accessible via the Internet may contain material that is illegal, defamatory, inaccurate or potentially offensive to some people.

3.4 Should an employee see any unacceptable materials or inappropriate use, he/she shall notify the site administrator or supervisor immediately. Report any instances where the Acceptable Use Policy or security may be violated. Report inappropriate Internet Web sites to the Technology Department so that access to the sites can be blocked in the future.

4.0 PROPER USE AND CARE

4.1 Before operating any equipment, users will be made familiar with the basics of safety and damage prevention, and trained on proper care and operation. Users will be individually assessed to determine their technical capabilities, and will be properly trained and supported by the Technology Department, as systems are issued for their use.

4.2 Many users, especially at school sites, will be sharing systems as part-time users. In this scenario, subsequent users will suffer if systems are misconfigured or damaged by previous users. In some cases, special software is used to protect

essential system configurations, requiring each user to log-on individually, and enabling only the services for which the user is authorized.

4.3 Equipment abuses are unacceptable whether out of frustration, misuse, negligence or carelessness. Users are responsible for damage to or loss of district equipment. District vandalism policies apply, making users liable for intentionally inflicted damage.

4.4 Users should not attempt repairs without authorization or support from designated District or school site personnel. Volunteers, parents, family members, or friends are not authorized to attempt repairs on District equipment.

4.5 Guidelines for the care and use of computer software are similar to hardware policies. Users are responsible for damage to or loss of District software systems. District vandalism policies apply to software as well, making users liable for intentionally inflicted damage.

4.6 Users shall not install or modify applications without approval and support of the District Technology Department or designated technology teachers and support staff at school sites. Any unauthorized changes to systems, operating software, application software, or hardware configurations will be reversed when discovered by technology or instructional staff. File-sharing software cannot be installed or used on District computers for the purpose of illegally sharing copyrighted materials such as music, images and software. This type of software is often used to "pirate", or illegally copy, music across the Internet. These Napster-like software packages are distributed under many different names including Gnutella, WinMX, Kazaa, LimeWire, Morpheus, and others. The use of this type of software is illegal when used to share copyrighted material. The most common use is the illegal "swapping" of music encoded in the MP3 format and is a violation of U.S. copyright laws.

4.7 Users shall not download or install copyrighted software without proper licensing. Non-licensed software will be deleted.

4.8 Copyrighted material shall be posted online only in accordance with applicable copyright laws.

4.9 In order to ensure proper configuration and to safeguard network security and performance, users should not attach computers, printers, network equipment (including wireless access points), or other types of hardware to the District's network without prior approval and support of the Technology Department. Attaching personally owned technology equipment to District hardware or to the District network is not allowed. Any equipment found to be in violation of this policy will be immediately disconnected.

5.0 PERSONAL RESPONSIBILITY

5.1 All technology equipment is District property.

5.2 Employees shall not access, post, submit, publish, or display harmful or inappropriate content that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or disparagement of others.

5.3 Employees shall not use the system to promote unethical practices or any activity prohibited by law, Board policy, or administrative regulations.

5.4 Employees shall not use the system to engage in commercial or other for-profit activities without permission of the Superintendent or designee. In addition, District electronic resources cannot be used to conduct political or religious activities. District e-mail cannot be used to advertise or solicit for non-District sponsored events, activities or organizations.

5.5 The District maintains a public Internet site. Any information to be posted on the public Web site must be approved through administrators (or their designee) and the District's Technology Department. Principals must approve all postings on school Web pages. Restrictions apply to links to other sites that may not be appropriate and to personal information or pictures of students without parental consent.

5.6 Employees shall not attempt to interfere with other users' ability to send or receive email, nor shall they attempt to read, delete, modify, or forge other users' mail.

5.7 Employees shall not develop any classroom or work-related web sites, blogs, forums, or similar online communications representing the District or using district equipment or resources without permission. Such sites shall be subject to rules and guidelines established for District online publishing activities including, but not limited to, copyright laws, privacy rights, and prohibitions against obscene, libelous, and slanderous content. Because of the unfiltered nature of blogs any such site shall include a disclaimer that the District is not responsible for the content of the messages. The District retains the right to delete material on any such online communications.

5.8 Users shall report any security problems or misuse of the services to the Superintendent or designee.

5.9 The Technology Department will take an active role in backing up data on the servers. However, statistics show that backups usually don't restore correctly. Therefore, ultimately each staff member is responsible for backing up their own data in at least two different locations to ensure that their data is not lost (i.e., on computer locally, on server, and/or external storage device, etc.). The Technology Department will take an active role in monitoring the disk space on all servers. Users who are taking up a greater than average amount of disk space will be notified and educated in storage management.

6.0 SECURITY AND PASSWORDS

6.1 To maintain security, users are issued unique User ID's and passwords to enable their access. Do not use other people's passwords. Do not tell others your password

including staff of the Technology Department. If it is known that you have shared your password with anyone else you will be required to change it. Do not write down a password where others can see it, and change passwords regularly as recommended by the Technology Department.

7.0 PENALTIES FOR VIOLATIONS

7.1 Violation of the Acceptable Use Policy may result in a reduction or loss of access privileges. In many cases, access privileges may be essential to job functions. Additionally, those failing to follow the guidelines contained in this regulation may face disciplinary action.

8.0 EMPLOYEE ACKNOWLEDGEMENT

8.1 All employees of the District who have access to district technology will be required to annually acknowledge that they have received, read and accepted this Administrative Regulation.

Adoption Date: December 11, 2017

Code: EHAA-E

LARAMIE COUNTY SCHOOL DISTRICT NO. 2

EMPLOYEE ACKNOWLEDGEMENT

I have received, read **and** accept the guidelines in the Policies EHAA and EHAA-E on Employee Acceptable Use of Technology.

Print Name: _____

Dept/Site_____

_____

Signature

Date: _____