Mary M. Knight School District
2987 W. Matlock-Brady Road
Elma, WA 98541

360.426.6767 (office)
360.427.5516 (fax)

www.marymknight.com

Dear Parents,

Mary M. Knight School has the ability to enhance your child's education through the use of computers and access to the Internet. The Internet represents a network of information available through the use of a computer. The Internet allows your child the opportunity to reach out to many other resources, share information, learn concepts, etc. Your child may be communicating with other students or adults from other parts of the world at no added, direct expense to you (e.g., phone bills, on-line time charges, service) in order to do research for school related projects. The district does not provide Internet access for personal use. It is intended solely as a tool to improve our educational resources.

It is very important that electronic communications be written appropriately. Therefore, the messages should not contain profanity, obscene comments, sexually explicit material, and expressions of bigotry, racism or hate. Also, they should not contain personal information that you would not want any stranger to have such as your name, address or phone number.

With this educational opportunity also comes responsibility. It is important that you and your child read the ethics code and discuss it together. When your child is given an account number and allowed to use the computers, it is extremely important that the rules are followed. Accessing inappropriate material or expressing oneself inappropriately will result in the loss of the privilege to use this educational tool. The District has the capability to access your child's Internet history of visited sites while on any school computer.

Parents, remember that you are legally responsible for your child's actions. Please stress to your child the importance of using only his or her own account number and password and the importance of keeping it a secret from other students. Your child should under NO circumstances let anyone else use their account number and password, because the student who uses your child's account number may violate the terms of this agreement. Your child will be held responsible for maintaining the security of the account number.

Please take time to sit down with your child to read and discuss the Rules and Code of Ethics for Mary M. Knight School Computer Users. Then sign and return to us the statement provided as soon as possible.

A signed agreement must be on file before the student will be given the opportunity to access the Internet.

Sincerely,

Matthew J Mallery

Matt Mallery
Superintendent

INTERNET PARENT LTR

Procedure Electronic Resources and Internet Safety

K-20 Network Acceptable Use Guidelines/Internet Safety Requirements
These procedures are written to support the Electronic Resources Policy of the board of directors and to promote positive and effective digital citizenship among students and staff. Digital citizenship represents more than technology literacy. Successful, technologically-fluent digital citizens live safely and civilly in an increasingly digital world. They recognize that information posted on the Internet is public and permanent and can have a long-term impact on an individual's life and career. Expectations for student and staff behavior online are no different from face-to-face interactions.

Use of Personal Electronic Devices
In accordance with all district policies and procedures, students and staff may use personal electronic devices (e.g. laptops, mobile devices and e-readers) to further the educational and research mission of the district. School staff will retain the final authority in deciding when and how students may use personal electronic devices on school grounds and during the school day.

Network
The district network includes wired and wireless devices and peripheral equipment, files, and storage, e-mail and Internet content (blogs, websites, collaboration software, social networking sites, wikis, etc.). The district reserves the right to prioritize the use of, and access to, the network.

All use of the network must support education and research and be consistent with the mission of the district.

Acceptable network use by district students and staff include:

A. Creation of files, digital projects, videos, web pages and podcasts using network resources in support of education and research;
B. Participation in blogs, wikis, bulletin boards, social networking sites and groups and the creation of content for podcasts, e-mail and webpages that support education and research;
C. With parental permission, the online publication of original educational material, curriculum related materials and student work. Sources outside the classroom or school must be cited appropriately;
D. Staff use of the network for incidental personal use in accordance with all district policies and procedures; or
E. Connection of personal electronic devices (wired or wireless) including portable devices with network capabilities to the district network after checking with *(insert title of position, i.e., technology director, IT director, assistant superintendent)* to confirm that the device is equipped with up-to-date virus software, compatible network card and is configured properly. Connection of any personal electronic device is subject to all procedures in this document.

Unacceptable network use by district students and staff includes but is not limited to:

A. Personal gain, commercial solicitation and compensation of any kind;
B. Actions that result in liability or cost incurred by the district;
C. Downloading, installing and use of games, audio files, video files, games or other applications (including shareware or freeware) without permission or approval from the *(insert title of position)*;
D. Support for or opposition to ballot measures, candidates and any other political activity;
E. Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and changes to hardware, software and monitoring tools;
F. Unauthorized access to other district computers, networks and information systems;
G. Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks;
H. Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacturing);
I. Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material; or
J. Attaching unauthorized devices to the district network. Any such device will be confiscated and additional disciplinary action may be taken.

The district will not be responsible for any damages suffered by any user, including but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries or service interruptions caused by his/her own negligence or any other errors or omissions. The district will not be responsible for unauthorized financial obligations resulting from the use of, or access to, the district's computer network or the Internet.

Internet Safety
Personal Information and Inappropriate Content:

A. Students and staff should not reveal personal information, including a home address and phone number on web sites, blogs, podcasts, videos, social networking sites, wikis, e-mail or as content on any other electronic medium;
B. Students and staff should not reveal personal information about another individual on any electronic medium without first obtaining permission;
C. No student pictures or names can be published on any public class, school or district website unless the appropriate permission has been obtained according to district policy; and
D. If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.

Filtering and Monitoring
Filtering software is used to block or filter access to visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). Other objectionable material could be filtered. The determination of what constitutes "other objectionable" material is a local decision.

A. Filtering software is not 100 percent effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Every user must take responsibility for his/her use of the network and Internet and avoid objectionable sites;
B. Any attempts to defeat or bypass the district's Internet filter or conceal Internet activity are prohibited (e.g., proxies, https, special ports, modifications to district browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content);
C. E-mail inconsistent with the educational and research mission of the district will be considered SPAM and blocked from entering district e-mail boxes;
D. The district will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by minors to inappropriate material on the Internet is deliberate and consistent monitoring of student access to district devices;
E. Staff members who supervise students, control electronic equipment or have occasion to observe student use of said equipment online, must make a reasonable effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of the district; and
F. Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively.
G. The district will provide a procedure for students and staff members to anonymously request access to internet websites blocked by the district's filtering software. The procedure will indicate a timeframe for a designated school official to respond to the request. The requirements of the Children's Internet Protection Act (CIPA) will be considered in evaluation of the request. The district will provide an appeal process for requests that are denied.

Internet Safety Instruction
All students will be educated about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response:

A. Age appropriate materials will be made available for use across grade levels; and
B. Training on online safety issues and materials implementation will be made available for administration, staff and families.

Copyright
Downloading, copying, duplicating and distributing software, music, sound files, movies, images or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. However, the duplication and distribution of materials for educational purposes is permitted when such duplication and distribution falls within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

Ownership of Work
All work completed by employees as part of their employment will be considered property of the district. The District will own any and all rights to such work including any and all derivative works, unless there is a written agreement to the contrary.

All work completed by students as part of the regular instructional program is owned by the student as soon as it is created, unless such work is created while the student is acting as an employee of the school system or unless such work has been paid for under a written agreement with the school system. If under an agreement with the district, the work will be considered the property of the District. Staff members must obtain a student's permission prior to distributing his/her work to parties outside the school.

(continued on next page)

Network Security and Privacy

Network Security

Passwords are the first level of security for a user account. System logins and accounts are to be used only by the authorized owner of the account for authorized district purposes. Students and staff are responsible for all activity on their account and must not share their account password.

The following procedures are designed to safeguard network user accounts:

A. Change passwords according to district policy;
B. Do not use another user's account;
C. Do not insert passwords into e-mail or other communications;
D. If you write down your user account password, keep it in a secure location;
E. Do not store passwords in a file without encryption;
F. Do not use the "remember password" feature of Internet browsers; and
G. Lock the screen or log off if leaving the computer.

Student Data is Confidential

District staff must maintain the confidentiality of student data in accordance with the Family Educational Rights and Privacy Act (FERPA).

No Expectation of Privacy

The district provides the network system, e-mail and Internet access as a tool for education and research in support of the district's mission. The district reserves the right to monitor, inspect, copy, review and store without prior notice information about the content and usage of:

A. The network;
B. User files and disk space utilization;
C. User applications and bandwidth utilization;
D. User document files, folders and electronic communications;
E. E-mail;
F. Internet access; and
G. Any and all information transmitted or received in connection with network and e-mail use.

No student or staff user should have any expectation of privacy when using the district's network. The district reserves the right to disclose any electronic messages to law enforcement officials or third parties as appropriate. All documents are subject to the public records disclosure laws of the State of Washington.

Archive and Backup

Backup is made of all district e-mail correspondence for purposes of public disclosure and disaster recovery. Barring power outage or intermittent technical issues, staff and student files are backed up on district servers regularly. Refer to the district retention policy for specific records retention requirements.

Disciplinary Action

All users of the district's electronic resources are required to comply with the district's policy and procedures (and agree to abide by the provisions set forth in the district's user agreement). Violation of any of the conditions of use explained in the (district's user agreement), Electronic Resources policy, or in these procedures could be cause for disciplinary action, including suspension or expulsion from school and suspension or revocation of network and computer access privileges.

Adoption Date:
Classification:
Revised Dates: **06.01; 06.08; 06.11; 02.12; 06.15**

Internet Use Agreement Form

STUDENT

I understand and will abide by the district's *Internet Use Agreement*. I further understand that any violation of these regulations is unethical and may constitute a criminal offense. Should I commit any violation of this agreement, my access privileges may be revoked, disciplinary action may be taken, and/or appropriate legal action may be taken.

User Name:
(Please Print) _____ **Grade:** _____

Signature: _____ **Date:** _____

(If you are under the age of 18, a parent or guardian must also read and sign this agreement.)

PARENT OR GUARDIAN

As the parent or guardian of this student, I understand the *Internet Use Agreement* and realize that this access is designed for educational purposes. I also recognize it is impossible for Mary M. Knight School District to restrict access to all controversial materials, and I will not hold it responsible for materials acquired on the network. I hereby give permission for my child to access the Internet and certify that the information contained on this form is correct.

Parent or
Guardian's Name:
(Please Print) _____

Signature: _____ **Date:** _____

SPONSORING TEACHER

I have read the *Internet Use Agreement* and agree to promote this agreement with the student. Because the student may use the network for individual work or in the context of another class, I cannot be held responsible for the student's use of the network. As the sponsoring teacher, I do agree to instruct the student on acceptable use of the network and proper network etiquette.

Teacher's Name:
(Please Print) _____

Signature: _____ **Date:** _____