# Electronic Resources

### 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 privately owned electronic devices to the district wireless network determined by acceptance of the wireless network use policy posted on the district wireless guest login page.

**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 that are not directly related to instructional support or curriculum goals.
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. Attempts (successful or not) to gain unauthorized access to other district computers, networks and information systems;
G. Cyber bullying, 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.
K. Uploading, saving, and storage of personal videos, pictures, and/or audio files and installation of applications for personal use on district computers or file servers.

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 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

As required by OSPI, 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.

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.

All student work is copyrighted. Permission to publish any student work requires permission from the parent or guardian and distributed with school administrator permission.

## 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. See policy 5251 for more information.

## 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).

District employees shall not use a student name in the subject line or body of an e-mail. Initials or indirect reference to a student name is acceptable.

### 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 Adult Acceptable Use Affidavit and Student Acceptable Use Agreement/Parent Opt Out Form, 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: 2/5/96
Revised: 5/5/03
Revised for First Reading: 2/4/13
Second Reading and Adoption: 2/19/13

# Marysville School District

## Student Acceptable Use Policy/Parent Opt Out Form

### Introduction

We are pleased to offer students of Maryville School District access to the district computer network resources, electronic mail, and the Internet. Parents, please review this document carefully, with your son/daughter. Families have the right to restrict the use of Internet and e-mail by completing this form and returning it to your school. The request for restriction is recorded in the student information system, and the form is kept on file. Any questions or concerns about this permission form or any aspect of the computer network should be referred to your school's Library Media Specialist and/or building secretary. A copy of Board policy regarding student access to networked information resources (2022) and this document are available on the Marysville School District web site, www.msvl.k12.wa.us.

**OPT-OUTS remain in effect for the current school year.**
***If no documentation is on file, it will be assumed that permission for Internet and e-mail usage has been granted.***

### General Network Use

The network is provided for students to conduct research, complete assignments, and communicate with others. Access to network services is given to students who act in a considerate and responsible manner. Students are responsible for good behavior on school computer networks just as they are in a classroom or a school hallway. Access is a privilege - not a right, and entails responsibility. As such, general school rules for behavior and communications apply, and users must comply with district standards. Beyond the clarification of such standards, the district is not responsible for restricting, monitoring, or controlling the communications of individuals utilizing the network.

District staff may review files and communications to maintain system integrity and insure that users are using the system responsibly. Users should not expect that files stored on district servers will be private.

### Internet / E-mail Access

Access to the Internet and e-mail will enable students to use thousands of libraries and databases. Within reason, freedom of speech and access to information will be honored. Families should be warned that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate, or potentially offensive to some people. While our intent is to make Internet access available to further educational goals and objectives, students may find ways to access other materials as well. Filtering software is in use, but no filtering system is capable of blocking 100% of the inappropriate material available on the Internet. We believe that the benefits to students from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages. Ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the Marysville School District support and respect each family's right to decide whether or not to restrict access (see page 2).

### Publishing to the Internet

Parents, your daughter or son's work may be considered for publication on the Internet, specifically on his/her school's web site. The work will appear with a copyright notice prohibiting the copying of such work without express written permission. In the event anyone requests such permission, those requests will be forwarded to the student's parent/guardian.

Photos of students may be published on school/district websites, illustrating student projects and achievements. In addition, your daughter or son's full name may be considered for publication on his/her school's web site. If published, his/her name will appear on pages with a clear school related purpose and will be included to further instructional and/or co-curricular activities. Permission for such publishing does not grant permission to share any other information about your son/daughter beyond that implied by their inclusion on the web page(s). **If you do not want your child's work, photo or name to be published on the website**, please indicate this on the RESTRICTION OF RELEASE OF DIRECTORY INFORMATION, which can be found on the Student Emergency Information Card located in your students school office.

# Maryville School District
## Student Acceptable Use Policy/Parent Opt Out Form

Unacceptable network use includes but is not limited to:

- Sending, storing, or displaying offensive messages or pictures
- Using obscene language
- Giving personal information, such as complete name, phone number, address, or identifiable photo, without permission from teacher and parent or guardian
- Cyber bullying, hate mail, harassing, insulting or attacking others, discriminatory jokes and remarks
- Damaging or modifying computers, computer systems, or computer networks – downloading, installing, and using games, audio files, video files, or other applications including shareware or freeware
- Violating copyright laws
- Sharing or using others' logons or passwords or other confidential information
- Trespassing in others' folders, work, or files
- Intentionally wasting limited resources
- Posting information, sent or stored online, that could endanger others
- Employing the network for nonacademic or personal commercial or political purposes, financial gain, or fraud
- Attaching unauthorized equipment to the district network

Violations may result in a loss of access (Board policy and procedures 3200 on student rights and responsibilities). Additional disciplinary action may be determined at the building level. When applicable, law enforcement agencies may be involved.

**Parent/Guardian Opt Out:**

Check below if you DO NOT want your student to have access to one or more of the following:

______ e-mail systems

______ Internet

**OPT-OUTS remain in effect for the current school year.**
If no documentation is on file, it will be assumed that permission has been granted
for access to the Internet and e-mail usage.

Parent/Guardian Signature ______________________ ____________ Date _______________

Student Name ________________________________ School_____________________________ Grade_____

# Adult Acceptable Use Affidavit

**Printed Name:** ______________________________

**Birth Date (MMDDYYYY):**______________________________

1. **I hereby certify that I have read and understand the Electronic Resources Policy (No. 2022).**

   Signature ______________________________ Date ________________

2. **As a user of the Marysville School District (MSD) computer network, I certify that I have read and understand the Electronic Resources Procedures (No. 2022P) concerning the use of MSD network and computers to access networked computer services such as electronic mail and internet.**

   Signature ______________________________ Date ________________

3. **Furthermore, I understand that violation of the policy or procedures could result in the loss of privilege to use MSD computers or to access the MSD network and could also result in discipline up to and including termination of employment.**

   Signature ______________________________ Date ________________

4. **Furthermore, I understand that if I am in violation of the policy and procedures with respect to the use of any personal device, I assume all responsibility.**

   Signature ______________________________ Date ________________

**Job Type (mark one):**

○ **Certificated Employee**
○ **Certificated Substitute**
○ **Other** ______________________________
○ **Classified Employee**
○ **Classified Substitute**
○ **Student Teacher**
○ **Personal Services Contract**

Building ______________________________ Assignment______________________________

Student Teacher or Substitute for______________________________

Start Date ____________________ End Date ____________________

**Requesting Administrator Signature** ______________________________

---

## Human Resources Use ONLY

**Domain/Email User ID Assigned** (LLLLLFMDD): ______________________________

**Password** (MMDDYYYY): ______________________________

Revised 2/2013