



Mount Vernon School District Technology Appropriate Use Guidelines

Purpose of Appropriate Use Guidelines

The purpose of these guidelines is to provide guidance to students and staff in the use of technology in order to maximize the derived benefits, provide safety when using technology, and ensure the security of confidential information. These guidelines apply to all district staff members and students and cover the district's K20 electronic network.

I. Use of District-Owned Electronic Communication Devices

A. General

The purpose of district-owned technology resources is to enhance the educational experience of students and to increase the operational efficiency of staff. Practices that attempt to achieve this purpose in a safe, legal manner are acceptable while practices that do not attempt to achieve this purpose, or are unsafe or detrimental, are considered not acceptable.

Internet users are encouraged to find resources that meet their individual needs and take advantage of many useful functions of the network. There are many applications that can be used in an educationally beneficial manner as well as applications that can be used in an inappropriate, illegal, or unacceptable manner. New applications and websites are being developed every day including instant messaging, blogging, social networking, and online collaboration tools. The district will establish a baseline of filtered websites across all schools. Individual school staffs may choose to filter additional sites.

It is possible that students may find material on the Internet that parents consider objectionable. Although the district has deployed an Internet filtering system and students are supervised when they use the Internet, this does not guarantee that students will not access inappropriate materials. While it is the responsibility of teachers to instruct students in network safety and appropriate use, it is the responsibility of students to use technology resources appropriately. District guidelines for accessing the Internet prohibit access to material that is inappropriate in the school environment. Students should report inappropriate access of material to a teacher, other staff person, or their parents. Parents are encouraged to discuss responsible use of the Internet with their children at home and how this responsibility extends to using the Internet at school.

The Mount Vernon School District believes that technology and network-based tools are important for 21st Century learning and MVSD expects all of its students to have fair and equitable access to these resources while at school. We are an "opt-out" district. Parents should contact their school administrators if they do not want their child using the filtered Internet or district-provided network resources at school.

Installation of unapproved equipment (i.e. wireless access points, routers, switches, network cabling), unapproved or unlicensed software, or changing of district required parameter settings can have detrimental effects on both the educational experience and the operation of technology. It is therefore important that only approved equipment and software be installed, and district required settings not be changed or bypassed.

Acceptable

- Creation of files, projects, videos, web pages and podcasts using network resources for educational and administrative purposes
- Use of network resources such as email, chat, blogs, wikis, and websites in a school appropriate manner
- Installation of appropriately licensed and approved software on district technology

Unacceptable

See school handbooks governing student discipline.

The following uses of the K20 network are unacceptable and may result in suspension or revocation of network privileges. Unacceptable use is defined to include, but not be limited to, the following:

- Violation of School Board Policies (2022 & 2022P Electronic Resources; 2025 & 2025P Copyright Compliance; 3027 & 3027P Prohibition of Harassment, Intimidation and Bullying; or 3220 & 3220 Freedom of Expression) or any provision in the student handbook.
- Transmission of any material in violation of any local, state, or federal law. This includes but is not limited to: copyrighted materials not covered by fair use provisions, threatening or obscene material, or material protected by trade secret.
- The use of profanity, obscenity, or other language that may be offensive to another user.
- Any form of vandalism, including but not limited to damaging hardware, computer systems, or networks, and/or disrupting the operation of the network.
- Copying and/or downloading commercial software or other material, e.g. music, in violation of federal copyright laws.
- Use of the network for financial gain, commercial activity, or illegal activity, e.g. hacking.
- Use of the network for political activity (Washington RCW 42.17.130, Use of public agency or agency facilities in campaigns).
- Use of the network to access pornographic or obscene material.
- Creating and/or placing a computer virus on the network.

- Accessing another person's individual account without prior consent or accessing a restricted account without the prior consent of the responsible administrator or teacher. The person in whose name an account is issued is responsible at all times for its proper use. Passwords should never be shared with another person and should be changed frequently. Passwords should not be common words or names that can be found in a dictionary.
- Posting information or images that could be a form of harassment or could promote a negative culture in the school environment by causing a student to feel uncomfortable or unsafe at school.
- Activity with a malicious intent to disrupt the network.
- Installation of unlicensed or unapproved software.
- Installation of unapproved technology on the network (i.e. wireless access points, routers or switches not provided or approved by the Teaching and Learning/Technology Departments).
- By-Passing of District specified filtered Internet websites or using proxy sites to bypass District filtering on computers used by students

B. Guidelines for Students

Student Safety and Privacy

The school district has an obligation to protect student safety and to balance this with the need for open communications when using the Internet. Students who are inappropriately identified via the Internet can become subjected to unhealthy situations or unwelcome communications.

The purposes of these guidelines are:

- To inform all users of the possible dangers of allowing students to publish identifying information on the Internet;
- To recognize that there are potential advantages of allowing students to publish identifying information on the Internet;
- To inform all users that online activities of students will be monitored;
- To inform all users that all students must be provided with instruction on appropriate online behavior including interacting with other individuals on social networking websites and in chat rooms, and cyber bullying awareness and response; and
- To provide schools with a recommended set of guidelines governing how student-identifying information should be allowed in publishing on the Internet.

Student users of the MVSD K20 network should be aware that information accessed, created, sent, received, or stored on the network is not private. It is subject to review by network system administrators who may investigate complaints regarding inappropriate or illegal material. (See Student Acceptable Use Policy for specific list of rights and responsibilities.)

Copyright & Plagiarism

Adherence to federal copyright law is required in both the print and the electronic environments. MVSD Board Policy states the District intent to adhere to the provisions of Public Law 94-553 and subsequent federal legislation and guidelines related to the duplication and/or use of copyrighted materials. MVSD guidelines only permit copying materials specifically allowed by copyright law, fair use guidelines, license agreements, or proprietor's permission. Additional copyright and fair use information can be found at:

- U.S. Copyright Office - Fair Use
- Stanford Copyright & Fair Use - Fair Use
- Copyright and Fair Use - Information & Library Services - UMUC

Acceptable

- Use of copyrighted material with author permission
- Use of copyrighted material that meets the fair use criteria

Unacceptable

- Using network resources to commit plagiarism.
- Unauthorized use, copying, or forwarding of copyrighted material.
- Unauthorized installation, use, storage, or distribution of copyrighted software.

C. Guidelines for Staff

The Internet/Intranet is a vast resource capable of providing enhanced information gathering and communication skills to assist in educational and employment-related endeavors.

Acceptable

Use of the Internet/Intranet is appropriate under all of the following circumstances:

- Support of the academic program;
- Telecommunications;
- Association and union activities; and
- Reasonable personal use to the extent that such use does not violate any express prohibitions of contracts and agreements and does not interfere with the staff members' assigned duties and responsibilities.

Unacceptable

- Use of the network for financial gain, commercial activity, or illegal activity, e.g. hacking. Use of the network for political activity. (Washington RCW 42.17.130 Use of public agency or agency facilities in campaigns.
- Use of District resources to contact students for non-educational purposes or any other purpose not in furtherance of the goals of the District.

All staff members are encouraged to develop the necessary skills to use the Internet/Intranet effectively and efficiently.

Staff members are expected to teach responsible use to students when they access the Mount Vernon School District K20 Network and the Internet, as well as provide guidance and supervision of students. Specifically:

- Teachers and other supervising adults will monitor student use, and provide students with instruction on Internet safety, including appropriate online behavior, in particular interacting with other individuals on social networking websites and in chat rooms, and cyber bullying awareness and response.
- District-owned technology that allows access to the Internet by students should only be placed in areas where adults are available to monitor.

Staff members who meet their professional responsibility as outlined above shall be protected from any potential liability.

There is no legitimate expectation of privacy in electronic mail communications. Each staff member will be provided with a password for accessing the Internet/Intranet and electronic mail. Staff members should maintain confidentiality with regard to their passwords; however, it is understood that the Employer will have access to all passwords. The district will maintain passwords in a safe and confidential location where access to such passwords by students and third parties is as secure as possible.

Email Guidelines - Staff Email Accounts

General

- All staff members are issued an email account.
- Others may be issued Guest Accounts based on their need for doing MVSD business after completing an application to the Human Resources Department.
- Email users are expected to use commonly accepted practices. Messages should not contain large attachments, large embedded graphics, or such a long recipient list as to cause difficulty for the district email server.

Acceptable

- Using email to fulfill the responsibilities of the position in which employed.
- Incidental personal use, meaning that staff may from time-to-time use district property (telephones and e-mail) for personal communication, as long as it will not interfere with district operations, and that will not be a discredit to the district.

Unacceptable

- Violation of Washington RCW 42.17.130 on political activity
- Violation of Washington Law, School Board Policy, District Administrative Rules.
- The use of vulgar and/or plainly offensive, obscene, or sexually explicit language in any form.
- Copying commercial software or other material in violation of federal copyright laws.
- Use of the network for financial gain, commercial activity, or illegal activity.
- Accessing another person's individual account without prior consent or accessing a restricted account without the prior consent of the responsible administrator or teacher.
- Sharing of inappropriate materials or their sources with students or other adults or knowingly accessing inappropriate materials

II. Use of Personal Electronic Communication Devices at School

The district will not be responsible for loss or damage of personal technology brought to school by students. Students assume responsibility for all lost, damaged, or stolen personal technology devices. Student cell phones shall be turned off during class time unless specifically allowed by the teacher. Unacceptable use of personal electronic communication devices may result in suspension or revocation of personal device privileges.

Acceptable

- Personal devices such as cell phones, handhelds, digital cameras, MP3 players, and laptops may be used for instructional purposes in the classroom at the discretion of the teacher. The same personal devices may be used outside of the classroom at the discretion of the school.
- Use of network resources such as email, chat, blogs, and Internet websites in a school appropriate manner.

Unacceptable

- Use of a personal device that violates any of the unacceptable uses for district-owned technology listed above.
- Use of a personal device to gain or give an advantage in a testing situation.

- Use of personal devices during class that are not approved by the school or the individual teacher, e.g. cell phones, MP3 players.
- Downloading and installing district licensed software on personal devices unless specifically allowed by the licensing agreement.