

MONTPELIER EXEMPTED VILLAGE SCHOOLS

Technology, Computer Network and Internet

USER ACCEPTABLE USE POLICY (AUP)

The Montpelier Exempted Village School District recognizes that as telecommunications and other technologies shift the ways in which information may be accessed, communicated and transferred by members of the society. Methods of instruction and student learning will also change. The district generally supports access by its staff and students to rich information resources to analyze and evaluate such information. In a free and democratic society, access to information is a fundamental right of citizenship.

Goals and General Principals

1. This Acceptable Use Policy is an extension of the school district's Student Code of Conduct and Board Policy.
2. In order for the school district to be able to continue to make its information resources available, all users must take responsibility for appropriate and lawful use of network access and other technology. Users must understand that one person's misuse of technology, may jeopardize the ability of all users to access the network and the internet.
3. The district firmly believes that the valuable information and interaction available using technology far outweighs the possibility that users may procure material that is not consistent with the educational goals of the district.
4. There will be no expectation that every student will have a laptop or personal computing device. All guidelines set forth by the Acceptable Use Policy apply to the Personal Computing Device Policy.

District Responsibilities

1. The District Technology Coordinator or his/her designee, will serve as the coordinator to oversee the use of District technology systems.
2. All District staff members are responsible for the dissemination of this Acceptable Use Policy and will work with schools to enforce this policy.
3. The District reserves the right to revise this Acceptable Use Policy as it deems necessary and will post the current policy on its web site as notice to users of any revisions. Users are responsible for reading the policy regularly.

User Responsibilities

1. Users are responsible for good behavior on school computer networks just as they are in a classroom or other school facilities.
2. Various technology, the network and telecommunication equipment is provided for students and staff to conduct research and communicate with others.
3. General school rules for behavior and communications apply to the use of technology.
4. Access to various technology and network services will be provided to students and staff who agree to act in a considerate and responsible manner.

Listed below are provisions regarding appropriate and responsible use of technology, the computer network and the Internet. If you have any questions about these provisions, you should contact a building administrator, immediate supervisor or other personnel designated by the district. If any user violates this policy, the user's access may be denied or withdrawn and he/she may be subject to additional disciplinary action.

I. Guidelines for Acceptable Use

The main principles defining "acceptable use" are those stated above: to use computing facilities only for the academic purpose for which they are provided, to show consideration to other users, to respect the privacy of all other users and to obey all relevant guidelines.

- New users are required to review the AUP. Appropriate user accounts will be created upon the completion and return of the appropriate AUP signature page.
 - a) Appendix A – Student Signature Page
 - b) Appendix B – Staff Signature Page
- Users, and if appropriate, the user's parents/guardians, will be required to review the AUP annually. User accounts will be maintained upon the completion and return of the appropriate AUP signature page. (Appendix A)
- Users may use the equipment available in any of the laboratories, if the laboratories are not being used for a class.
- Users are not to unreasonably deprive other users of access.
- Users are not to occupy a terminal for excessive periods if other people are waiting.
- All users are responsible for immediately reporting any damage or malfunction of any hardware, software, security or other component of network systems to proper administration or faculty.

- Users may use personal computers and other electronic computing devices upon the return of a completed Student User of Personal Electronic Device Agreement. Use of personal computing device follows the same guidelines as school computer when connected to the network. (Appendix B.)

II. Privacy

Technology, including network access and internet access, is provided as a tool for student education. In order to maintain system integrity, the school district reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and internet access and any and all information transmitted or received in connection with such usage. All such information shall be and remain the property of the School District and no user shall have any expectation of privacy regarding such materials.

III. Use of Computer Software and Operating Systems

Computer software has been purchased for school use only and is protect by Federal Copyright Laws. The following guidelines apply to the use of software purchased by The Montpelier Exempted Village Schools.

1. Treat computer software like any other copyrighted material.
 2. You may not install software protected by copyright on any school computer without written permission from the technology coordinator, media coordinator or district superintendent.*
 3. You may not install computer software purchased by The Montpelier Exempted Village Schools on any computer outside of the school district.**
 4. You may not attempt to modify, reprogram, translate, disassemble, decompile or otherwise reverse engineer any software protected by copyright laws.
 5. Software residing on privately owned computers must be personally owned, except in the case of antivirus software and desktop monitoring software used by the School District
 6. Software companies will not be held liable for any indirect, special, incidental, economic or consequential damages arising from the use or inability to use the software.
 7. Unauthorized reproduction or distribution of software or information protected by copyright laws or any portion of them may result in severe civil and criminal penalties and may be prosecuted to the maximum extent possible under the law. Furthermore, violations of the above guidelines will result in applicable disciplinary actions and financial charges to remove such software from the computer's hard drive at a charge comparable to current industry standards for service work.
- * Software purchased by school staff for home use may not be installed on school computers unless the license agreement allows for such use.
- ** Some exceptions do exist; please contact the technology coordinator for more information regarding software titles in question.

IV. Unacceptable Use of Technology and/or Network

The smooth operation of any network relies upon the proper conduct of the end-users, who must adhere to strict guidelines. The school district is providing access to its computer networks and the Internet for only educational purposes. If you have any doubt about whether a contemplated activity is educational, you may consult with the person(s) designated by the school to help you decide if a use is appropriate. In general, user responsibilities require efficient, ethical and legal utilization of the network resources. The use of network resources must be in support of the educational goals of the Montpelier Exempted Village School District. Uses deemed inappropriate include but are not limited to the following:

- Using obscene language or sending or displaying offensive messages or pictures
- Harassing, insulting or attacking others
- Plagiarism and violation of copyright laws
- Downloading of copyrighted music is forbidden
- Engage in scholastic dishonesty
- Damaging electronic devices or computer networks
- Disrupting the intended use of electronic resources
- Using others' accounts or unauthorized access to network resources
- Intentionally wasting limited resources
 1. Users shall not tie up the network with idle non-educational activities.
 2. Users shall not play non-educational games on school owned computers.
 3. Users shall not store information, pictures, sounds or movies on school owned computers that do not support the educational goals of the Montpelier Exempted Village Schools.
- Using electronic resources for commercial and non-educational purposes
 1. Users will not use the Internet for advertising, promotion, commercial purposes or similar objectives.
 2. Users will not use the Internet to conduct for-profit business activities or to engage in religious activities.
 3. Users are also prohibited from engaging in any non-governmental-related fund raising or public relations activities such as solicitation for religious purposes, lobbying for political purposes or soliciting votes.

4. The District is not responsible for any other commercial activity users engage in.
- Vandalizing information – includes, but is not limited to:
 1. The uploading, downloading or creation of computer viruses
 2. Attempting to harm or destroy district equipment or materials
 3. Changing settings on electronic equipment without authorization
 - Revealing personal information about anyone without written permission
 - Violating the law or encouraging others to violate the law through the use of technology

V. Student Safety and CIPA

While school staff will make reasonable efforts to supervise the use of technology including the network and internet, it is impossible to supervise at all times. The Montpelier Exempted Village School District has taken available precautions to restrict access to controversial materials. However, on a global network it is impossible to control all materials and users may discover controversial information.

The Children's Internet Protection Act (CIPA) was signed into law on December 21, 2000. Under CIPA, no school or library may receive discounts unless it certifies that it is enforcing a policy of Internet safety that includes the use of filtering or blocking technology (see below). This Internet Safety Policy must protect against access, through computers with Internet access, to visual depictions that are obscene, child pornography or (in the case of use by minors) harmful to minors. The school or library must also certify that it is enforcing the operation of such filtering or blocking technology during any use of such computers by minors.

General Principles

1. This AUP shall govern all electronic activity, including e-mail and access to the Internet, which is undertaken by district employees, students and parents/guardians. No user may engage in activities prohibited by this policy. All use will be in compliance with the acceptable use provisions of the Internet service provider.
2. Internet access and the use of e-mail through the use of the school's system are provided for educational purpose. The term "educational purpose" learning activities both in school and at home, employee professional or career development, and communication between teachers, students and their parents. If any user has a question whether their Internet usage is consistent with the district's educational purpose, goals and mission, they should consult with the appropriate supervisor, principal, teacher, etc.
3. The District shall implement Internet filtering software in an attempt to block user access to inappropriate and/or harmful material on the Internet. Objectionable content is pre-determined by the District. When the software finds any such objectionable content, it denies the user access to the site based on the level of access granted to the user by the District. Filtering technology is not perfect and therefore, may interfere with legitimate educational research. In the event that the filtering software is unsuccessful and children gain access to inappropriate and/or harmful material, the District will not be liable. (See Appendix C for Filtering Policies)
4. The District reserves the right to monitor all online activities including internet access and all e-mail. Such monitoring may lead to discovery that the user has violated or may be violating. The school, either by itself or in combination with the Data Acquisition Site providing Internet access, will utilize filtering software or other technologies to prevent students from accessing visual depictions that are (1) obscene, (2) child pornography or (3) harmful to minors. The School will also monitor the online activities of students, through direct observation and/or technological means, to ensure that students are not accessing such depictions or any other material which is inappropriate for minors. Internet filtering software or other technology-based protection systems may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by students age 17 and older. The term "harmful to minors" is defined by the Communications Act of 1934 (47 USC Section 254 [h][7]), as meaning any picture, image, graphic image file or other visual depiction that:
 - taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex or excretion;
 - depicts, describes or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts or a lewd exhibition of the genitals;
 - taken as a whole, lacks serious literary, artistic, political or scientific value as to minors.
5. The District specifically reserves the right to revoke access and/or take other appropriate disciplinary action, with respect to any user who violates this policy. The District reserves the right to terminate any user's access to the Internet, including access to e-mail, at any time and for any reason. If a student's access is revoked, the District will ensure that the student nonetheless continues to have a meaningful opportunity to participate in the educational program.

Educational Use of the Internet

1. When using the Internet for class activities, teachers should:
 - Select material that is appropriate in light of the age of the students and that is relevant to the course objectives.
 - Preview the materials and sites they require students to access to determine the appropriateness of the material contained on or accessed through the site.
 - Provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly.
 - Assist their students in developing the skills to ascertain the truthfulness of information, distinguish fact from opinion and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.
2. As appropriate, the District will provide students and parents with guidelines and instructions for student safety while using the Internet.
3. The District Internet Acceptable Use Policy contains restrictions on accessing inappropriate material and student use generally will be supervised. However, there is a wide range of material available on the Internet, some of which may or may not fit the particular values of the students. It is not practically possible for the District to monitor and enforce a wide range of social values in student use of the Internet. Further, the District recognizes that parents bear primary responsibility for transmitting their particular set of family values to their children. The District will encourage parents to specify to their child(ren) what material is and is not acceptable for their child(ren) to access through the District system.

Student Safety

1. All users and their parents/guardians are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged pupils. Every user must take responsibility for his or her use of the computer network and Internet and stay away from these sites. Parents of minors are the best guide to which materials should be avoided by their children. If a student finds that other users are visiting offensive or harmful sites, he or she should report such use to personnel designated by the school district.
2. Student photographs and personal contact information. The school must obtain written parental consent prior to the disclosure of student information or student work on any District Web page
 - a. The school and its staff will not post or transmit photographs and personal contact information about students without prior written parental consent from the parent of the student whose information is being posted.
 - b. Student users will not post or transmit photographs and personal contact information about themselves or other students without prior written parental consent from the parent of the student whose information is being posted.
 - c. Parental consent must be delivered to the child's teacher or principal and kept on file for as long as the photograph and personal information are posted. It may be required for a parent or guardian to provide consent for each posting or transmission of personal information about their child. Personal contact information includes, but is not limited to, home address, telephone number, school name, school address and classroom.
3. Student users will not agree to meet with someone they have met online without their parent's approval and participation.
4. Student users will promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.
5. Users are responsible for the use of their individual accounts and should take all reasonable precautions to prevent others from being able to use their accounts. Under no conditions should a user provide their password to another person, except that supervisors and/or teachers may require users to provide their passwords.
6. Student users will immediately notify a teacher if they identify a possible security problem (such as disclosure of their password to another person) and other users will immediately notify the system administrator. No users will go looking for security problems, because this may be construed as an illegal attempt to gain access.
7. Restrictions against inappropriate language apply to public messages, private messages and material posted on Web pages.
 - Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, abusive or disrespectful language. Users will not post information that could interfere with the educational process or cause a danger of disruption in the educational environment. Users will not engage in personal attacks, including prejudicial or discriminatory attacks.
 - Users will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending messages, they must stop.
 - Users will not knowingly or recklessly post false or defamatory information about a person or organization.

8. Users should not repost a message that was sent to them privately without permission of the person who sent them the message.
9. Users should not post private information about another person.

VI. Online Communities and Cyber Bullying

Cyber bullying is the act of harassment that takes place via some method of technological media. If a student is being harassed and the effect is on the school it does not matter where the offense originates, even if off grounds, if the effect of such acts makes a transition to school grounds it is under our best judgment to take appropriate action.

- Cyber bashing, bullying or defaming of students and/or faculty is probationary and could lead to a dismissal from school.
- It is unacceptable to use computing and communication services (e.g., electronic mail and network news) to propagate abuse or any other material that contravenes the Discrimination Laws or Harassment Laws (or is otherwise insulting, rude, abusive or offensive)
- Impersonating anyone and creating an online profile for this individual is a form of dishonesty and is therefore, probationary and could lead to a dismissal from school.
- Violating school expectations (this includes the times when school is out of session) will in all likelihood result in disciplinary consequences, including suspension from school and may effect any leadership position a student may have or is making application for.
- If you are going to post photos of faculty or staff, be sure to ask permission of the individuals in your photograph

VII. School Web Pages

1. The District superintendent will designate a District Web Publisher, responsible for maintaining the official District web page and monitoring all District web activity. The Web Publisher will develop style and content guidelines for official District and school web page materials
2. Material placed on the web site is expected to meet academic standards of proper spelling, grammar and accuracy of information.
3. All Web pages should have a link at the bottom of the page that will help users find their way to the appropriate home page.
4. Teachers will be encouraged to establish Web pages for use with class activities or to provide a resource to students, parents and other teachers.
 - Teachers will be responsible for maintaining their class or educational resource sites. Teacher web pages will not be considered official material, but will be developed in such a manner as to reflect well upon the District.
5. Support Staff will be encouraged to develop web pages that provide a resource for others.
 - Support staff will be responsible for maintaining their resource sites. Staff web pages will not be considered official material, but will be developed in a manner as to reflect well upon the District.
6. Students may be encouraged to create a web site as part of a class activity. Material presented on a student class activity web site must meet the educational objectives of the class activity.
 - The District has the right to exercise control over the content and/or style of student web pages so long as its actions are reasonably related to legitimate pedagogical concerns.
 - Schools have the right to remove student web pages at the end of each school year.
7. Organization Web Pages
 - With the approval of the superintendent or building principal, extracurricular organizations may establish web pages.
 - Material presented on the organization web page must relate specifically to organization activities.
8. Web Pages shall not:
 - Contain personal contact information about students beyond that permitted by the school, district and parent.
 - Display photographs, videos or other images of any identifiable individual, other than a historical or public figure, without a signed release.
 - Contain advertisements for profit-making entities, such as publishers or other consumer goods purveyors, unless the site being linked to is predominantly instructional in nature (such as museum sites, encyclopedias, national parks, aquariums, literary organizations, etc.). The districts may not directly benefit financially from any entities linked to on their web pages.
 - Contain personal, non-educationally-related information.

VIII. Email Usage

1. Users will check their e-mail frequently and delete unwanted messages promptly.
2. "Acceptable" e-mail activities are those that conform to the purpose, goals and mission of the District and to each user's job duties and responsibilities. Users shall have no right to privacy while using the District's internet or e-mail system.
3. "Unacceptable" use is defined generally as activities using BOE hardware, software or networks at any time that does not conform to the purpose, goals and mission of the BOE and to each user's job duties and responsibilities. The following list, although not inclusive, provides some examples of unacceptable uses:
 - E-mail may not be used for personal purposes during working hours, except that users may engage in minimal e-mail activities for personal purposes, such as family correspondence, if the use does not diminish the employee's productivity, work product or ability to perform services.
 - Using e-mail services for private commercial or business transactions and any activity meant to foster personal gain.
 - Using school e-mail address to subscribe to websites or other internet services that do not conform to district educational activities.
 - Conducting non-District of Education fund raising or public relations activities such as solicitation for religious and political causes or not-for-profit activities.
 - Transmitting threatening, offensive harassing information (messages or images) containing defamatory, abusive, obscene, pornographic, sexually oriented, racially offensive or otherwise biased, discriminatory or illegal material.
 - Attempting to subvert network security, impair functionality of the network or bypass restrictions set by the network administrators. Assisting others in violating these rules by sharing information or passwords.
 - Distributing "junk" mail, such as chain letters, advertisements or unauthorized solicitations.
 - Revealing, publicizing, using or reproducing confidential or proprietary information regarding the DOE including, but not limited to, financial information, databases and/or the information contained therein, computer network access codes, staff or student information and business relationships.
 - Users should contact their supervisors about questionable e-mail usage.

IX. Use of Personal Electronic Devices

Students will be allowed to use personally owned computing devices to access the school's wireless network. This wireless access by personally owned devices is to be used as a means to enhance the student's education experience. Use of these devices in the school setting may be approved on a limited basis. Students are to use these devices in a responsible, efficient, ethical and legal manner. The administration reserves the right to determine if a student's use of personal electronic communication devices is inappropriate and/or disrupts the learning environment and may take appropriate disciplinary action, including but not limited to, confiscation of the device, which will be returned to the student and/or parent(s)/guardian(s) in accordance with established building guidelines. For this policy a Personal Electronic Device is defined as an electronic communication device capable of internet access, word processing and other school-related applications. This may include:

- Notebook or Netbook Computer
- iPad or other Tablet Computer
- iPod Touch and other small internet devices
- iPod, Zune, Sansa or other digital media player

Use of cell phones or any of these devices for non-scholastic communication during the school day is strictly prohibited during school hours.

Permission to bring and use personal devices is contingent upon adherence to the following guidelines.

1. Access to the District's wireless network will only be granted upon return of the Electronic Device Usage Agreement. An authorization label for approved access will be placed on the laptop and must always be visible for use at school.
 - a. Other connections to the internet will not be allowed. Examples would include 3G or 4G provided by Verizon, AT&T or any other provider.
2. Personal Computing Devices must meet the following criteria:
 - a. Acceptable OS – Windows XP (Any Version), Windows Vista (Any Version), Windows 7 (Any version)
 - b. iPad and Android 3.0 upon release of appropriate application to allow monitoring of usage.
 - c. Computer must be setup with user accounts. The log-in/user name MUST include student's name. (NO Nicknames)
 - d. Computer Name must include user's last name. (NO nicknames)
 - e. Approved antivirus / security protection software installed.

3. Users must allow district technology staff to install desktop monitoring software on Personal Computing Devices. ***This software will only be used to monitor devices attached to the schools network.***
4. Students shall have no expectation of privacy once they have been authorized to connect to the District's Electronic Network.
5. The District may examine the laptop and search its contents if there is reason to believe that school policies or guidelines have been violated.
6. The personal owner is the only person authorized to use the electronic device. Siblings may share a computer only if the computer is setup to use separate user accounts for each student.
7. The use of an electronic device is solely limited to support the instructional activities currently occurring in the instructional environment.
8. Permission to use electronic devices and charging of the devices in any instructional area, including but not limited to classrooms, will be at the sole discretion of the supervising adult and/or classroom teacher.
9. Use of electronic devices in common areas will be allowed but subject to the restrictions stated in the district policies. If a student appears to be in violation of any district policy, staff members should refer to the Student Policy Manual.
10. Safeguarding personal electronic devices and/or laptops is the sole responsibility of the user. The school district is not responsible for any loss or damage to the student's computer, including but not limited to losses or damage caused by hardware failure, data loss or the incurring of a virus.
11. Software residing on privately owned computers must be personally owned, except in the case of antivirus software and desktop monitoring software used by the District
12. Responsibility for the maintenance and repair of the equipment rests solely with the student/owner. District technicians will not service or repair any computer not belonging to the District. No internal components belonging to the District shall be placed in any personal equipment, whether as enhancements, upgrades or replacements. No software that is deemed by the Technology Department to be for personal use will be supported under any circumstances.

Consequences of Inappropriate and/or Prohibited Use

Failure to follow the acceptable use procedures contained in this policy will result in the loss of the privilege to use these tools and may result in school disciplinary action and/or legal action. The school district may deny, revoke the use of personal electronic devices or suspend access to the district network at any time. Additional consequences may result from any violation of the BOE policy for student behavior found in the student agenda.

Personal Electronic Device Security Risks

1. Laptops and other portable electronic devices are especially vulnerable to loss and theft. These items may be targeted in school, on school grounds, parking lots and on buses.
2. The student must be responsible and aware of all risks. Montpelier Exempted Village Schools will not accept responsibility for loss, damage, theft or non working personal property. Students who bring personally owned items on school property must assume the total responsibility of these items. Laptops and all other portable or digital electronic items that are lost, stolen or damaged are the responsibility of the student and their parents or guardians. As per BOE policy, administrators will not search for lost or stolen items. The school system and school system personnel cannot attempt to repair, correct or are responsible for malfunctioning personal hardware or software.
3. Laptops, netbooks and all other portable electronic devices should NEVER be left unattended for ANY period of time by the owner. When not in use they should be at the student's side or in secured location such as a school locker when applicable. If a laptop is found unattended, it will be turned into the school administration.

X. Failure to Follow Policy

Use of the any school owned electronic media is a privilege, not a right. A user violates this policy by his or her own action or by failing to report any violations by other users that come to the attention of the user. Further, a user violates this policy if he or she permits another to use his or her account or password to access the computer network and Internet, including any user whose access has been denied or terminated. Any user who violates this policy may have one or more of the following sanctions imposed:

- Loss of access to network resources until a signed User Agreement and in the case of a student a signed Parent/Guardian Agreement is returned to the Montpelier Exempted Village School District.
- Vandalism may result in the District seeking financial restitution
- When applicable, law enforcement agencies may be involved
- The School District may take other disciplinary action if deemed necessary.

District Liabilities

The School District makes no warranties of any kind, either expressed or implied, in connection with its provisions of access to and use of its computer networks and the internet provided under this policy and agreement. It shall not be responsible for any claims, losses, damages or costs (including attorney's fees) of any kind suffered, directly or indirectly, by any user or by a student's parent(s) or guardian(s) arising out of the user's use of its computer networks or the Internet under this policy. By agreeing to this policy, users are taking full responsibility for their use. The parent(s) or guardian(s) of students are agreeing to hold harmless the school, the District and all of their administrators, teachers and staff from any and all loss, costs, claims or damages resulting from the user's access to its computer network and the Internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user. The user and the user's parent(s) or guardian(s) agree to cooperate with the school in the event of the school's initiating an investigation of a user's use of his or her access to the computer network and the Internet, whether that use is on a school computer or on another's outside the District's network.