



Monty Tech Acceptable Use Standards

Monty-Tech Acceptable Use Policy (AUP)

This document is a guide to acceptable use of the Montachusett Regional Vocational Technical School (MRVTS) data communications network. It is intended to address the minimum standards of use for the data communications network as implemented at the Montachusett Regional Vocational Technical School. Access to data communications carried across other networks is subject to acceptable use policies of those other networks. If other networks are accessed through the MRVTS network, the more restrictive and/or conservative policy shall, in all cases, apply, without exception.

Acceptable use refers to whether the use of the data communications network is consistent with the guidelines established for each network, local area network, workstation or other data communications application, which the traffic traverses. Given the volatile nature of the technology employed and the demand that users make of networks, determining acceptable use is a dynamic and interactive process. The intent of this use policy is to make clear certain cases, which are consistent or inconsistent with the purposes of the MRVTS data communications network. It is not possible to enumerate all such possible uses.

1 Primary Goals

The MRVTS data communications network has the capacity to link workstations, local area networks and/or other external networks as well as access a wide variety of data communications resources worldwide. The goal of the MRVTS data communications network is to support and enhance instruction, research activities, and administrative records management among the staff and students of MRVTS as well as other interested parties who may participate with the express invitation and permission of the Montachusett Regional Vocational Technical School District, by providing access to computer mediated communication resources, shared resources, unique resources, and the opportunity for collaborative work. In addition to access to local shared resources, the MRVTS data communications network maintains high-speed access to the Internet, providing connections to regional, national and international resources. The following guidelines establish minimum standards with regard to all uses of the MRVTS data communications network.

2 Acceptable Use Policy

2.1 All use of the MRVTS data communications network must be consistent with MRVTS's primary Goals.

2.2 This policy shall be updated as conditions warrant. The most current version shall be posted on the MRVTS web site.

2.3 The System Manager (Director of Technology) may, at any time, make determinations that particular uses are or are not consistent with the purposes of the MRVTS data communications network. Such determinations will be reported, via electronic mail, posting to our home page, and/or message, to the user community.

2.4 The MRVTS data communications network shall only be used for legal purposes.

2.5 It is important that disruptions to the MRVTS data communications network be minimized. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer worms and/or viruses, and using the network to make unauthorized entry to any other machine or device accessible via the network. Recreational computing, game playing, participating in

non-educational chat rooms, social networks, and similar activities are considered unacceptable since such activities degrade system performance and/or denies access to other users.

2.6 Users may only access those areas to which they have been given authorization. Users should not attempt to access information which is not in their purview. This especially applies to administrative database information concerning the staff and students of MRVTS. If there are any questions concerning access, they should be directed to the System Manager.

2.7 Proper professional standards of conduct must be maintained. Users should refrain from transmitting any material which might be construed as threatening, obscene, or harassing. Users should refrain from accessing material which is inappropriate to the educational environment.

2.8 MRVTS does not endorse or permit access to material which may be considered educationally inappropriate or objectionable in nature. Access to such material on MRVTS owned workstations shall be restricted to the greatest extent possible; free speech and open scholarly research issues notwithstanding. MRVTS employs content filtering systems which provide the most technologically current protection available. MRVTS may not be held responsible for access to inappropriate and/or objectionable material from systems connecting to the MRVTS data communications network though outside telephone, cable or other data communications lines or on MRVTS workstations which have been intentionally reconfigured to bypass content filtering.

2.9 Information and resources accessible via the MRVTS data communications network are private to the individuals and organizations which own or hold the rights to those resources and information unless specifically stated otherwise by the owners or holders of such rights. Access to information or resources (even when that information or those resources are not securely protected) may occur only with prior permission of the owners or holders of such rights to those resources or information. Within resources residing on equipment owned, leased or otherwise contracted by MRVTS the final authority regarding specifically authorized rights to view and or access applications, files and other resources that reside on the system shall be the System Manager.

2.10 The MRVTS data communications network should only be utilized for approved activities. Profit making activities or use by for-profit institutions except when engaged in open scholarly communication and research shall only occur with the express permission of the System Manager.

2.11 MRVTS shall not assume liability for payment of any new subscriptions, royalties or other fees associated with accessing commercial services, bulletin board systems and/or databases without the prior express permission of the System Manager. In the event MRVTS is billed for such unauthorized access, the user shall be held accountable and may be required to reimburse MRVTS for charges accrued due to such unauthorized access.

2.12 Account codes and passwords are confidential and should not be shared with any other person without the permission of the System Manager.

2.13 Professional standards of conduct and ethics must be maintained with regard to the use of copyrighted and licensed software. It should be noted that it is illegal to duplicate copyrighted and licensed software for use by others.

2.14 Only software that directly supports approved curriculum may be installed on MRVTS workstations without the express permission of the System Manager.

2.15 Under no circumstances shall unlicensed software be installed on any MRVTS workstation.

2.16 Personal workstations (laptops and other equipment not owned or leased by MRVTS) may only be connected to the MRVTS data communications network (including wireless access points) with prior permission of the System Manager. Said workstations and other equipment approved for connection must meet certain configuration, operating system and virus protection standards. This section does not preclude certain access points (for example, the Performing Arts Center) temporarily being made available to the public.

3 Enforcement of Policy

3.1 User accounts and passwords may be used to administer networked workstation configuration, including but not limited to, restricting access to 'control panels', and the right to view or otherwise access certain directories and files on local workstations.

3.2 All files (including e-mail) enjoy full security and privacy privileges associated with the accounts to which they are assigned. No staff member or student shall access email or the accounts or

files of another person without the consent of the staff member/student, or the Superintendent-Director, or the Superintendent-Director's designee. Violations may be subject to disciplinary action. Privacy privileges notwithstanding, the Montachusett Regional Vocational Technical School District retains the right as owner and employer to examine any and all files residing on our systems as may be warranted to ensure compliance with this policy, satisfy records requests of law enforcement agencies or for other legitimate reasons. Random examination of web browser cache and history files may occur without notice.

3.3 Software is routinely employed which monitors and decodes network traffic.

3.4 Procedures are in place to insure compliance with Massachusetts Public Records regulations as they relate to e-mail (see section 6).

3.5 A log of all external web based traffic is maintained.

4 Violation of Policy

4.1 The System Manager of MRVTS and/or appropriate representatives of the Montachusett Regional Vocational Technical School District will review all alleged violations of the MRVTS Acceptable Use Policy. Violations of this policy will result in appropriate actions being taken.

4.2 In addition to this section, inappropriate computer use violations by students may be addressed by the Dean of Students in a manner consistent with other inappropriate behavior as defined in the Student Handbook. Inappropriate computer use violations by staff may be addressed by the Principal and/or System Manager.

4.3 Unauthorized access or attempt to access the administrative database files of the MRVTS shall be dealt with to the full extent of the law.

4.4 Any effort to conceal the history of computer use by the deletion, erasure or other attempts to remove files, including the installation and use of any program designed to hide evidence of Internet use, shall be deemed willful and malicious destruction of school property.

4.5 Any effort to bypass content filtering or to perform activities not related to education may result in disciplinary action.

4.6 Any misuse of our e-mail system, including the proliferation of spam and other unauthorized messages, are considered a violation of the Acceptable Use Policy.

5 Internet Safety Policies & CIPA Compliance

5.1 MRVTS shall maintain content filtering/blocking software which is updated at regular intervals. At present, filtering resides on the MRVTS network gateway and not on individual workstations (see section 5.5).

5.2 Inappropriate sites discovered to be accessible should be reported to the System Manager. Such sites may be blocked immediately by the System Manager. Conversely, blocking of sites which are necessary for "bona fide research" may be temporarily disabled.

5.3 Web links and/or references to the Montachusett Regional Vocational Technical School from other web sites which contain inappropriate or objectionable content shall be discouraged by whatever administrative means are available. This particularly applies to personal web pages of our staff and students.

5.4 Monitoring of Internet use shall be accomplished by a combination of staff supervision, the 'history files' associated with web browsers, monitoring of network traffic and the 'log' files of gateway.

5.5 Any MRVTS owned or leased workstation which will be used to access the Internet without going through the MRVTS network gateway shall be configured to employ appropriate content blocking and the user shall agree that such configuration will not be altered. This includes MRVTS workstations which are used off premises.

6 E-Mail Policies

6.1 MGL c 4 § 7 (Massachusetts Public Records Law) applies to all government records generated, received, or maintained electronically, including computer records and electronic mail.

6.2 MGL c 66 § 10 requires e-mail of our employees be available for inspection. All employees are expected to maintain suitable "mailboxes" in their e-mail accounts to comply with this requirement.

6.3 MGL c 66 § 8 requires that an e-mail archive be kept for a period of 7 years. All incoming and outgoing e-mail of all "@montytech.net" accounts (both staff and students) is archived.

6.4 In order to insure that Monty Tech is in compliance with records keeping regulations and acceptable practices, all e-mail correspondence related to an employee's job must be conducted using the employee's official "@montytech.net" e-mail account.

6.5 In order to insure our ability to comply with the Federal Rules of Civil Procedure Rules 26 and 34, employees may not use personal e-mail to conduct any school related business.

6.6 Content filtering/blocking is used to block access to personal e-mail accounts.

7 Disclaimer of Liability

7.1 The Montachusett Regional Vocational Technical School disclaims all liability for the content of material that a student may access on the Internet, for any damages suffered in the course of or as result of the student's Internet use, and any other consequences of a student's use. of the MRVTS data communications network.

7.2 By accepting and using a Monty Tech Computer Account and Password you agree not to: (a) upload, transmit, post, email or otherwise make available to any MRVTS workstation any content or other material in any format that is false, inaccurate, unlawful, harmful, threatening, abusive, harassing, tortious, defamatory, vulgar, obscene, invasive of another's privacy, libelous and/or otherwise objectionable; (b) infringes on any third party's intellectual property; or (c) contains viruses, worms, Trojan horses, corrupted files, or any other similar software or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment. You agree that you will not transmit or access any data that infringes any patent, trademark, trade secret, copyright or other proprietary rights of any party and agree to indemnify and hold harmless Montachusett Regional Vocational Technical School District from their claims if you do.

Version 9.2 - 25 April 08

Version 9.3 - 17 June 09

Version 9.4 - 7 January 2011

Version 9.5 - 2 April 2013