

MT. GILEAD EXEMPTED VILLAGE SCHOOL DISTRICT
TECHNOLOGY RESOURCES
ACCEPTABLE USE POLICY
Staff

Mt. Gilead Exempted Village School District Technology Resources include, but are not limited to, computers, file servers, laptops, software, e-mail, video equipment, AV equipment, public address systems, presentation equipment, telephones, voice mail systems, digital cameras, scanners, the local area network, the wide area network, and all equipment related thereto (collectively, "Technology Resources" or individually, "Technology Resource"). These resources are school property, purchased with public funds or grant monies, and are intended solely for use in furtherance of the mission of the District, to enhance the delivery of education, and to conduct necessary school business. Technology Resources may only be used for appropriate curricular and co-curricular purposes.

This policy sets forth the proper and acceptable uses of Technology Resources, electronic mail and communications and the Internet for school employees. The use of any Technology Resource shall constitute acknowledgment and acceptance by the user of this policy and all other applicable Mt. Gilead Board of Education policies and regulations.

Technology Resources and assigned network access, Internet access and e-mail access passwords are tools provided to school employees to assist in the performance of their job responsibilities and should be treated accordingly. Any school employee who violates this policy, or allows others to do so, may have his/her user access privileges revoked and shall be subject to disciplinary action, up to and including termination of employment. Any employee who is licensed by the State Board of Education may be subject to disciplinary action by the State Board for any use of technology that constitutes unprofessional conduct under the Licensure Code of Professional Conduct for Ohio Educators (adopted March 11, 2008). Each employee must sign a form to acknowledge he/she has read, understands and will comply with this Technology Resources Acceptable Use Policy. These forms will be kept on file by the District as binding legal documents.

The Mt. Gilead Board of Education reserves the right to modify this policy at any time. The Mt. Gilead Board of Education may pursue criminal prosecution or civil action for any unauthorized use of Technology Resources or any violation of this policy when appropriate.

Technology Resources and Acceptable Use Policy Outline

- A. General Standards of Conduct for Use of Technology Resources**
 - B. General Standards of Conduct for Electronic Mail and Communications**
 - C. General Standards of Conduct for Internet Use**
 - D. District Web Sites**
 - E. Disclaimers**
 - Form: Employee Receipt and Acknowledgment**
-

A. General Standards of Conduct for Use of Technology Resources:

1. Only software licensed to the Mt. Gilead Board of Education and/or authorized in writing by the Technology Director , or his or her designee, shall be installed on Technology Resources. Installation of such software shall be performed only by authorized personnel to ensure that the software is (a) compatible with existing computer systems; (b) properly installed, maintained, used and upgraded; (c) free from any computer virus; and (d) properly licensed. Installation of any other software, including but not limited to, shareware, freeware, public domain or demonstration copies of software, shall be installed with written permission by the Technology Director and the Academic Services Director or his/her designee. Unscheduled audits of Technology Resources will be periodically performed and any unlicensed or unapproved software will be removed without notice.
2. Only hardware licensed to the Mt. Gilead Board of Education and/or authorized in writing by the Technology Director , or his or her designee, shall be installed on Technology Resources. Installation of such hardware shall be performed only by authorized personnel to ensure that the hardware is (a) compatible with existing computer systems; (b) properly installed, maintained, used and upgraded; (c) free from any computer virus; and (d) properly licensed. Installation of any other hardware, including but not limited to, CPUs, motherboards, hard-drives, video cards, memory, CD-ROMs, DVD-ROMs, SCSI cards, modems/routers, network routers is prohibited. Memory based recording devices/media used for the transportation of information or enhancement devices (e.g., USB drives, cameras) are permitted. The District reserves the right to inspect or restrict such use should these devices/media contain material that could damage Technology Resources (e.g., viruses, malware, spam, spyware). Unscheduled audits of Technology Resources will be periodically performed and any unlicensed or unapproved hardware will be removed without notice. Technical support will not be provided for employee-owned hardware.
3. Technology Resource users shall not delete any software on the District's computers, copy any software owned by the District, or remove any hardware from the District's property without prior written permission from the Technology Director .
4. Technology Resource users may not deploy or install wireless access points or network routers.
5. Network and system passwords ensure the security of critical and sensitive electronic data and are the first defense against unauthorized access. Only passwords issued by the Technology Director, or his or her designee, shall be used. Technology Resource users are prohibited from divulging their passwords to other individuals. Habitual loss or unauthorized disclosure of any password shall be subject to disciplinary action.
6. Disruption of electronic services and interference with Technology Resources or electronic information (including but not limited to, uploading or downloading damaging data or illegal software; tampering with hardware or software; vandalizing or destroying data; introducing or

using computer viruses, worms or Trojan horses; or attempting to gain access to restricted information or networks) are prohibited.

7. Authorized users are prohibited from allowing any unauthorized person to use or operate any Technology Resource. Non-employees in the school for a specific purpose may be authorized by the Technology Director, or his or her designee, to use Technology Resources only under the direction and direct supervision of a school employee. Technology Resource users should shut down and secure in an appropriate fashion Technology Resources which are not in use.
8. Any use of Technology Resources to facilitate illegal activity is prohibited. Technology Resources shall not be used to encourage or promote any activity prohibited by law or Mt. Gilead Board of Education policy, rules, procedures or regulations. Any misconduct or criminal activity discovered will be referred to appropriate authorities.
9. Use of the District's Technology Resources to access or transmit obscene, pornographic, political, religious or violent materials or to transmit materials likely to be threatening, offensive or objectionable is prohibited. Such prohibited materials include, but are not limited to, "hacking" materials; "cyberbullying" activities; racist material or hate literature; terrorism instructions/directions or other dangerous information; profane or vulgar materials; threatening or inflammatory language; false or defamatory materials; disparagement of others based on race, color, religion, national origin, veteran status, ancestry, disability, age, sex, or sexual orientation; and any materials that advocate violating other's rights. In the context of educational purposes, the District may allow research or investigation of some objectionable materials to allow students to be better prepared to recognize social harms and improve their ability to deal effectively therewith.
10. Use of Technology Resources for political, commercial or for-profit purposes, including fund-raising unless specifically authorized by the District administration, is prohibited.
11. Unauthorized access, use, modification, alteration, vandalism or destruction of Technology Resources or electronic information is prohibited. Any inappropriate use of Technology Resources that may hinder future use is prohibited. Technology Resource users are expected to respect the District's property and to follow any instructions from the Technology Director, or his or her designee, regarding maintenance and care of equipment. Technology Resource users must promptly notify the Technology Director of any need for service to Technology Resources.
12. Technology Resources may not be used in violation of copyright laws. Any copyrighted material placed on any system connected to the District network without the author's permission will be removed.
13. Technology Resources may not be used in violation of privacy laws and the unauthorized disclosure, use or dissemination of personally identifiable information concerning students is prohibited. All Technology Resource users are required to protect themselves and others by not issuing or releasing any personal or confidential information via Technology Resources.

14. The Technology Director may establish and enforce quotas for usage of available space on the District network. Technology Resource users are expected to remain within allocated disk space and delete e-mail or other materials which take up excessive storage space.
15. Technology Resource users must immediately notify the Technology Director if they identify any security problem.
16. The District administration reserves the right to limit the times of access and to establish priorities among competing acceptable uses of Technology Resources.
17. All remote access and use of Technology Resources shall also be subject to all applicable requirements of this policy.

B. General Standards of Conduct for Electronic Mail and Communications:

1. The General Standards of Conduct for Use of Technology Resources set forth above shall be equally applicable to electronic mail and messenger system use by all full time and part time school employees.
2. In order to prevent the introduction of viruses or other harmful data or software into the District's computers and network, extreme caution should be exercised before opening any attachments to any incoming e-mail. If an e-mail attachment is not expected, is from an unknown source, or is an executable file (ending with .EXE or .COM), the attachment should not be opened and should be deleted immediately.
3. Sending or forwarding unsolicited e-mail, chain letters or "spam" is prohibited. Global transmissions to large contact groups are also discouraged due to the strain placed on network resources.
4. E-mail and electronic communications are written records which can be duplicated and altered at will. E-mail and messenger systems are not confidential or private, and all school employees should exercise common sense and restraint in their use of not only e-mail and other forms of electronic communication. All users must be aware that use of Technology Resources for both business and personal reasons may constitute public records under state law.
5. The use of e-mail or electronic communications to convey student information is prohibited, whether during or after school hours and whether on or off the District's premises, unless secured and approved by the Information and Technology Department. Instructional staff and the District administration may authorize the release of directory information about students, as defined by Ohio law, for internal administrative purposes or approved educational projects and activities.
6. School employees shall not use personal Internet e-mail providers (e.g. Hotmail, Yahoo, Gmail, etc.) to obtain an e-mail address or to send or receive e-mail from Technology Resources.

C. General Standards of Conduct for Internet Use:

1. The General Standards of Conduct for Use of Technology Resources set forth above shall be equally applicable to all Internet use.
2. Internet access over the District network may be provided only to school employees, students, individuals enrolled in Adult Education classes, and volunteers, aides or other persons in the school for a specific school purpose when authorized by the Technology Director, or his or her designee. Student Internet access may be limited to specified times, as provided by the instructors and the District administration.
3. Internet access over the District network is available only to support learning, to enhance instruction and to assist in the administration of the District. Internet access is to be used in a responsible, ethical and legal manner. All school employees are responsible for their actions and communications on the Internet.
4. The District has implemented technology protection measures to block or filter materials which are obscene or harmful to minors. The District will restrict, to the extent practicable and technically possible, access to offensive information and materials. Because Internet access provides connections to computer systems located all over the world, the District cannot, however, control the content of all information and materials available on the District network.
5. The District administration will determine whether any use of the network is inappropriate or unauthorized, or whether any Internet information and materials are objectionable.
6. Instructional Staff should preview recommended sites and materials selected for inclusion in coursework. Sites should be appropriate in light of the age of the students and relevant to course objectives. Student Internet use must be carefully monitored by District staff or authorized individuals. District staff and authorized individuals are expected to enforce all rules pertaining to student computer and Internet use and, if any instructional staff member becomes aware of student violations, he/she is expected to stop the activity and inform appropriate District administrators.
7. All Technology Resource users must first report promptly to the department/building administrator and the Director of Technology and Information any inappropriate information or material they encounter when using the Internet or which they believe may be available based on Internet usage by other individuals.
8. Files downloaded from the Internet must be scanned with virus detection software, if available, before being viewed or opened.
9. Internet users are prohibited from accessing or retrieving any relay chat or other real-time or "live" communications unless there has been prior clearance by the Technology Director. However, live communication for District business reasons within the District network is permissible.

10. Internet peer-to-peer file sharing and torrent use are prohibited unless there has been prior clearance by the Technology Director. However, file sharing for District business reasons within the District network is permissible.
11. The downloading and installation of programs from the Internet is prohibited without the prior written approval of the Technology Director or designee. Unauthorized programs will be removed without notice.
12. Information obtained via the Internet is not always reliable and should be verified for accuracy, quality, and completeness.
13. Distribution of student information, using any personal Internet service provider, whether during or after school hours and whether on or off the District's premises, is a violation of student privacy and is subject to disciplinary action.
14. For curricular reasons only, authorized users may access personal sites/pages if they reflect the professional image of the District and are consistent with the mission of the District.

D. District Web Sites

The District has established a Web site, www.mtgilead.k12.oh.us, and will develop Web pages that present information about the District. The Superintendent, or designee, is responsible for maintaining the District Web site and shall establish Web Site Publishing Guidelines to manage the posting of information to the District Web site, the posting of any school, class or student Web pages, and the creation of links to or from outside sources. All Web sites and pages (including links) hosted on the District network must reflect the professional image of the District and be consistent with the mission of the District. Unauthorized Web sites, links, or pages may **not** be placed on the District network. The Superintendent, or designee, may remove any content from any technical resource which is determined to be detrimental to the District.

E. Disclaimers

The District does not guarantee the privacy of any information, including but not limited to e-mail messages or electronic communications or files sent or received via Technology Resources. Any person utilizing any Technology Resource understands and agrees that he/she is specifically waiving any expectations of privacy in communications, data and other information stored, displayed, accessed, communicated or transmitted thereon. The District reserves and will exercise the right to access, monitor, review, audit, log and intercept computer activity, Internet use, e-mail, electronic communications and other Technology Resource use by school employees at all times and without notice. The District may edit or remove any materials from Technology Resources which are determined to be objectionable. If an investigation is started, the staff member(s) will be notified. If any misconduct or criminal activity is discovered, the information or communications may be used to document such conduct and may be referred to the District administration and appropriate authorities. The use of a

File: EDE
Adopted: July 9, 1996
Revised November 16, 2010
Employee attachment to Policy

District provided password or code does not restrict the District's right to access, monitor, review, audit, log, and intercept electronic information or communications.

The District denies any responsibility for the accuracy, quality or completeness of any information available over the Internet. Furthermore, the District assumes no responsibility for any costs, liabilities or damages incurred through use of Technology Resources.

Technology Resource users are responsible for archiving and backing-up all electronic information and communications which need to be retained. The District makes no guarantee that the functions or services provided by or through the District network will be error free or without defect. The District is not responsible for any damages incurred due to loss of data or delays in or interruption of services.

The Technology Director may investigate any unusual activity involving Technology Resources and may periodically report to the Superintendent or designee on the manner in which Technology Resources are being used.