Manchester Local Schools

Acceptable Use Guidelines (AUG) for Technology Resources

Information for Employees

In accordance to Board Policy 7540.04, The Manchester Local School District (MLSD) provides technology resources to facilitate growth in productivity, communication, media literacy and collaboration. Use of technology, whether district owned or personal property, must support education, academic research, and be consistent with the educational objectives of the MLSD. Any other use is unacceptable.

The MLSD buildings offer access to the Internet via both wired and wireless network connections. This agreement and associated rules and regulations refer to all electronic computing, communications, recording and/or imaging devices – including but not limited to computers, tablets, cell phones, mobile devices, video conferencing, portable memory storage devices, cloud storage, digital cameras and all other technology infrastructure and software:

- *Owned by, leased by or on loan to the District or any third party engaged in providing services for the District.*
- *Any computing or telecommunications devices owned by, in the possession of or being used by district staff that are operated on the grounds of any district facility or connected to any equipment at any district facility by means of direct connection, telephone line or other common carrier type of connection including hardwired, fiber and/or wireless.*

This agreement is in effect for any school-sponsored activity at any time or any place.

The goals of these Acceptable Use Guidelines are to maximize the benefits of these technological resources for our school district, to encourage responsible behavior, and to protect students, staff and the community from potential harm.

General guidelines for use of technology by staff:

1. Do no harm.

2. Use technology…
   - To complete educational tasks and seek academic excellence.
   - To support academic research, class lessons and objectives.
   - In a manner consistent with the educational goals of the district.
   - In a manner consistent with student handbooks, staff handbooks, and Board Policy and guidelines. Maintain professional standards and conduct in all things related to technology, social media and electronic communications.

3. Respect and Protect…
   - Privacy of self and others.
   - Hardware, software and network resources.
   - Intellectual property rights.

Systems Monitoring
In accordance with the federal Childhood Internet Protection Act (CIPA), Internet access at MLSD is filtered. The use of technology resources may be monitored by authorized employees to protect the integrity of district technological resources as well as individual compliance with this policy. Administrators may examine and use data in disciplinary actions; evidence of crime will be provided to law enforcement officials.

Any district email is intended only for the addressee(s) and may contain material that is confidential under state and federal law. **School District email is to be used only for school purposes.** MLSD may monitor email to and from its network. Email and any responses may be archived for later retrieval and may constitute a public record and therefore may be made available upon request in accordance with Ohio Public Records law (ORC 149.43).

All staff members are expected to be familiar with and follow
Board Policy 7540.04 - STAFF TECHNOLOGY ACCEPTABLE USE AND SAFETY.

That policy is attached.
By signing this document, you are agreeing to follow all guidelines within that policy.
This includes policies on social media.

Penalties for Improper Use
The use of a MLSD account and district technology is a privilege, not a right, and misuse will result in disciplinary action appropriate to the seriousness of the offense and according to district disciplinary policy.

I have read, understand and agree to abide by the provisions of the Acceptable Use Guidelines of the Manchester Local School District

Date:_____

Employee Name:_____ **Signature:**_____

Disclaimer
MLSD makes no guarantees about the quality of the services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from use of the network or accounts.
AUG form is required for all staff that will be using district technology equipment or the network and will be kept on file.
Created: July 2013 Updated: June 2020

Policy Manual

STAFF TECHNOLOGY ACCEPTABLE USE AND SAFETY

Code

po7540.04

Adopted

February 18, 2003

Last Revised

January 8, 2019

7540.04 - **STAFF TECHNOLOGY ACCEPTABLE USE AND SAFETY**

Technology has fundamentally altered the ways in which information is accessed, communicated, and transferred in society. As a result, educators are continually adapting their means and methods of instruction, and the way they approach student learning, to incorporate the vast, diverse, and unique resources available through the Internet. The Board of Education provides Technology and Information Resources (as defined by Bylaw 0100) to support the educational and professional needs of its staff and students. The Board provides staff with access to the Internet for limited educational purposes only and utilizes online educational services/apps to enhance the instruction delivered to its students and to facilitate the staff's work. The District's Internet system does not serve as a public access service or a public forum, and the Board imposes reasonable restrictions on its use consistent with its limited educational purpose.

The Board regulates the use of District Technology and Information Resources by principles consistent with applicable local, State, and Federal laws, and the District's educational mission. This policy and its related administrative guidelines and any applicable employment contracts and collective bargaining agreements govern the staffs' use of the District's Technology and Information Resources and staff's personal communication devices when they are connected to the District's computer network, Internet connection and/or online educational services/apps, or when used while the staff member is on Board-owned property or at a Board-sponsored activity (see Policy 7530.02).

Users are required to refrain from actions that are illegal (such as libel, slander, vandalism, harassment, theft, plagiarism, inappropriate access, and the like) or unkind (such as personal attacks, invasion of privacy, injurious comment, and the like). Because its Technology Resources are not unlimited, the Board has also instituted restrictions aimed at preserving these resources, such as placing limits on use of bandwidth, storage space, and printers.

Users have no right or expectation to privacy when using District Technology and Information Resources (including, but not limited to, privacy in the content of their personal files, e-mails, and records of their online activity when using the District's computer network and/or Internet connection).

Staff members are expected to utilize District Technology and Information Resources to promote educational excellence in our schools by providing students with the opportunity to develop the resource sharing, innovation, and communication skills and tools that are essential to both life and work. The Board encourages the faculty to develop the appropriate skills necessary to effectively access, analyze, evaluate, and utilize these resources in enriching educational activities. The instructional use of the Internet and online educational services will be guided by Board Policy 2520 - Selection of Instructional Materials and Equipment.

The Internet is a global information and communication network that brings incredible education and information resources to our students. The Internet connects computers and users in the District with computers and users worldwide. Through the Internet, students and staff can access relevant information that will enhance their learning and the education process. Further, District Technology Resources provide students and staff with the opportunity to communicate with other people from throughout the world. Access to such an incredible quantity of information and resources brings with it, however, certain unique challenges and responsibilities.

First, the Board may not be able to technologically limit access, through its Technology Resources, to only those services and resources that have been authorized for the purpose of instruction, study and research related to the curriculum. Unlike in the past when educators and community members had the opportunity to review and screen materials to assess their appropriateness for supporting and enriching the curriculum according to adopted guidelines and reasonable selection criteria (taking into account the varied instructional needs, learning styles, abilities, and developmental levels of the students who would be exposed to them), access to the Internet, because it serves as a gateway to any publicly available file server in the world, opens classrooms and students to electronic information resources that may not have been screened by educators for use by students of various ages.

Pursuant to Federal law, the Board has implemented technology protection measures that protect against (e.g., filter or block) access to visual displays/depictions/materials that are obscene, constitute child pornography, and/or are harmful to minors, as defined by the Children's Internet Protection Act. At the discretion of the Board or Superintendent, the technology protection measures may also be configured to protect against access to other material considered inappropriate for students to access. The Board also utilizes software and/or hardware to monitor online activity of staff members to restrict access to child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors. The technology protection measures, may not be disabled at any time that students may be using the District Technology Resources, if such disabling will cease to protect against access to materials that are prohibited under the Children's Internet Protection Act. Any staff member who attempts to disable the technology protection measures without express written consent of an appropriate administrator will be subject to disciplinary action, up to and including termination.

The Superintendent or Director of Technology may temporarily or permanently unblock access to websites or online educational services/apps containing appropriate material, if access to such sites has been inappropriately blocked by the technology protection measures. The determination of whether material is appropriate or inappropriate shall be based on the content of the material and the intended use of the material, not on the protection actions of the technology protection measures. The Superintendent or Director of Technology may also disable the technology protection measures to enable access for bona fide research or other lawful purposes.

Staff members will participate in professional development programs in accordance with the provisions of law and this policy. Training shall include:

A. the safety and security of students while using e-mail, chat rooms, social media and other forms of direct electronic communications;

B. the inherent danger of students disclosing personally identifiable information online;

C. the consequences of unauthorized access (e.g., "hacking", "harvesting", "digital piracy", "data mining", etc.), cyberbullying and other unlawful or inappropriate activities by students or staff online; and

D. unauthorized disclosure, use, and dissemination of personally-identifiable information regarding minors.

Furthermore, staff members shall provide instruction for their students regarding the appropriate use of technology and online safety and security as specified above, and staff members will monitor students' online activities while at school.

Monitoring may include, but is not necessarily limited to, visual observations of online activities during class sessions; or use of specific monitoring tools to review browser history and network, server, and computer logs.

The disclosure of personally identifiable information about students online is prohibited.
Building principals are responsible for providing training so that Internet users under their supervision are knowledgeable about this policy and its accompanying guidelines. The Board expects that staff members will provide guidance and instruction to students in the appropriate use of the District Technology Resources. Such training shall include, but not be limited to, education concerning appropriate online behavior, including interacting with other individuals on social media including in chat rooms and cyberbullying awareness and response. All users of District Technology Resources are required to sign a written agreement to abide by the terms and conditions of this policy and its accompanying guidelines.

Staff will be assigned a school email address that they are required to utilize for all school-related electronic communications, including those to students, parents and other staff members.
Staff members are responsible for good behavior when using District Technology and Information Resources - i.e., behavior comparable to that expected when they are in classrooms, school hallways, and other school premises and school sponsored events. Communications on the Internet are often public in nature. The Board does not approve any use of its Technology and Information Resources that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines.

General school rules for behavior and communication apply.

Users who disregard this policy and its accompanying guidelines may have their use privileges suspended or revoked, and disciplinary action taken against them. Users are personally responsible and liable, both civilly and criminally, for uses of District Technology and Information Resources that are not authorized by this policy and its accompanying guidelines.
The Board designates the Superintendent and Director of Technology as the administrators responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to staff members' use of District Technology and Information Resources.

Social Media Use

An employee's personal or private use of social media may have unintended consequences. While the Board respects its employees' First Amendment rights, those rights do not include permission to post inflammatory comments that could compromise the District's mission, undermine staff relationships, or cause a substantial disruption to the school environment. This warning includes staff members' online conduct that occurs off school property including from the employee's private computer. Postings to social media should be done in a manner sensitive to the staff member's professional responsibilities.

In addition, Federal and State confidentiality laws forbid schools and their employees from using or disclosing student education records without parental consent. See Policy 8330. Education records include a wide variety of information; posting personally identifiable information about students is not permitted. Staff members who violate State and Federal confidentiality laws or privacy laws related to the disclosure of confidential student or employee information may be disciplined. Staff members retain rights of communication for collective bargaining purposes and union organizational activities.

Legal

P.L. 106-554, Children's Internet Protection Act of 2000

47 U.S.C. 254(h), (1), Communications Act of 1934, as amended (2003)

20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003)

18 U.S.C. 1460

18 U.S.C. 2246

18 U.S.C. 2256

20 U.S.C. 6777, 9134 (2003)

47 C.F.R. 54.500 - 54.523