

## **Manchester Local School District (AUP)**

### *Computer Network and Internet Acceptable Use Policy (Public Access)*

This document constitutes the School District's Computer Network and Internet Acceptable Use Policy ("Policy"), and applies to all persons who use or otherwise access the Network and/or Internet, whether with District or personal equipment or whether on-site or by wireless or other remote access ("Users").

1. Purpose and Use: The School District is providing Guest access to its Network. Access to system computers and the Network is a privilege, not a right. The District reserves the right to withdraw access at any time for any lawful reason.
2. Users Bound by Policy in Accepting Access: The User consents to the terms of this Policy whenever he or she accesses the Network. Users of the Network are bound to the terms of this Policy regardless of whether or not a copy was received and/or signed for by the User.
3. Personal Responsibility: Users are responsible for their behavior on the Network. Each User is responsible for reading and abiding by this Policy and any and all future amendments.
4. Reporting Misuse of the Network: Users must report any misuse of the Network to the District administration. "Misuse" means any apparent violation of this Policy or other use which has the intent or effect of harming another person or another person's property.
5. Violating Policy with Personal Equipment: The use of personal equipment and/or personal Internet access to violate this Policy or to assist another to violate the Policy is prohibited. Exceeding permission (such as abusing access to unfiltered Internet connectivity) is a violation of this Policy.
6. Waiver of Privacy: By accepting Network access, Users waive any and all rights of privacy in connection with their communications over the Network or communications achieved through the use of District equipment or software. Electronic mail (e-mail) and other forms of electronic communication (including instant messaging of all forms and SMS messages originating from email) are not guaranteed to be private. The District owns all data in the system. Systems managers have access to all messages for purposes of monitoring system functions, maintaining system efficiency, and enforcing computer/network use policies and regulations, District policies, and state and federal laws. Illegal activities or suspected illegal activities may be reported to the authorities.
7. Unacceptable Uses of the Network: All Users must use the Network in an appropriate and responsible way, whether their specific actions are described in this Policy or not. Examples of unacceptable uses include, but are not limited to, the following

\*OFFENSIVE OR HARRASSING ACTS: Creating, copying, viewing, transmitting, downloading, uploading or seeking sexually explicit, obscene, or pornographic materials. Using language inappropriate to the school environment, including swearing, vulgarities or language that is suggestive, obscene, profane, abusive, belligerent, harassing, defamatory or threatening. Making, distributing or redistributing images, jokes, stories or other material that would violate this Policy or the School District's harassment or

discrimination policies, including material that is based upon slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, sexual orientation, or other protected characteristics. Engaging in harassment, stalking, or other repetitive unwanted communication or using the Internet in support of such activities.

**\*VIOLATIONS OF PRIVACY:** Unauthorized copying, modifying, intruding, or attempts to copy, modify or intrude, into the folders, files, data, work, networks, passwords or computers of others, or intercepting communications intended for others. Copying, downloading, uploading, or transmitting student or School District confidential information.

**\*CREATING TECHNICAL PROBLEMS:** Knowingly performing actions that cause technical difficulties to the system, other users or the Internet. Attempting to bypass school Internet filters or to “hack” into other accounts or restricted information. Uploading, downloading, creating, or transmitting a computer virus, worm, Trojan horse, or other harmful component or corrupted data. Attempting to hack, alter, harm, destroy or interfere with the normal operation of software, hardware, data, other District Network resources, or using the District Network or to do any of the same acts on the Internet or outside Networks. Downloading, saving, and/or transmitting data files large enough to impede the normal functioning of the computer or the Network (such as many music, video, image, or software files) unless given permission by the System Administrator. Moving, “repairing,” reconfiguring, reprogramming, modifying, or attaching any external devices to Network equipment, computers or systems without the permission of the System Administrator. Removing, altering, or copying District software for personal use or for the use of others.

**\*VIOLATING LAW:** Actions that violate state or federal law or encourage others to do so. Offering for sale or use, soliciting the purchase or provision of, or advocating the use of any substance that the possession or use of is prohibited by law or District Policy. Seeking information for the purpose of creating an explosive device or biohazard, or communicating or seeking materials in furtherance of criminal activities, terrorism, or other threatening acts.

**\*VIOLATING COPYRIGHT:** Uploading, downloading, copying, redistributing or republishing copyrighted materials without permission from the owner of the copyright. Users should assume that materials are protected under copyright unless there is explicit permission for use.

**\*POLITICAL USE:** Creating, transmitting or downloading any materials that support or oppose the nomination or election of a candidate for public office or the passage of a levy or a bond issue. Soliciting political contributions through the Network or conducting any type of official campaign business.

**\*GENERAL MISCONDUCT:** Using the Network in a manner inconsistent with the expectations of Manchester Local Schools for the conduct of guests in the school environment. Uses that improperly associate the School District with Users’ personal activities or to activities that injure the District’s reputation. Uses that mislead others or violate the standards of academic or personal integrity, including but not limited to plagiarism, disseminating untrue information about individuals or groups, or using another’s password or some other user identifier.

8. System Security and Integrity: The District reserves the right to suspend operations of the Network, in whole or in part, at any time for reasons of maintaining data security and integrity or any other lawful reason. The District reserves the right to block or filter any web sites, e-mail addresses, servers or Internet domains which it, in its sole judgment, has determined to present a risk of exposing students or employees to sexually explicit or otherwise inappropriate content, or which exposes the system to undue risk of compromise from the standpoint of security or functionality.

9. No Warranties Created: By accepting access to the Network, you understand and agree that the School District, any involved Information Technology Centers, and any third-party vendors make no warranties of any kind, either expressed or implied, in connection with provision of access to or the use of the Network. They shall not be responsible for any claims, losses, damages or costs (including attorneys' fees) of any kind suffered, directly or indirectly, by any student or employee arising out of that User's use of and/or inability to use the Network. They shall not be responsible for any loss or deletion of data. They are not responsible for the accuracy of information obtained through electronic information resources.

Legal Ref.: Ohio Rev. Code 3313.20, 3313.47, 3319.321

Children's Internet Protection Act of 2000, 47 USC § 254 (h), (l)

Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g