

POLICY

BOARD OF EDUCATION MONROE TOWNSHIP

PROGRAM

2361/Page 1 of 6

ACCEPTABLE USE OF DISTRICT ELECTRONIC NETWORK, COMPUTERS, AND RELATED RESOURCES

Acceptable Use of District Electronic Network, Computers, and Related Resources

Purpose

The Board recognizes that as telecommunications and other new technologies shift the manner in which information is accessed, communicated and transferred those changes will alter the nature of teaching and learning. Access to telecommunications will allow users to explore databases, libraries, the Internet, interactive communication areas, and the like while exchanging information with individuals throughout the world. The Board supports access to information sources but reserves the right to limit in school use to material appropriate to educational purposes. The Board directs the Superintendent to effect training of teaching staff members in skills appropriate to analyzing and evaluating such resources as to appropriateness for educational purposes.

The Board provides access to the district electronic network, computers and related resources for educational purposes only. The Board retains the right to restrict or terminate user access to the district electronic network, computers and related resources at any time, for any reason. The Board retains the right to have district personnel monitor network activity, in any form necessary, to maintain the integrity of the network and insure its proper use.

Internet Safety and Protection

The school district is in compliance with the Children's Internet Protection Act and has addressed specific methods for compliance with Regulation 2361. Technology protection measures for all computers in the district are installed that block and/or filter visual depictions that are obscene as defined in section 1460 of Title 18, United States Code; child pornography, as defined in section 2256 of Title 18, United States Code; are harmful to minors including any pictures, images, 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; or depicts, describes, or represents in a patently offensive way, with respect to serious literary, artistic, political or scientific value as to minors. Notwithstanding blocking and/or filtering the visual depictions prohibited in the

Children's Internet Protection Act, the Board shall determine other Internet material that is inappropriate for minors.

An Internet Safety Plan, which reflects the district Regulation 2361 compliance measures will be made available to all parents/guardians and staff. These procedures address access by minors to inappropriate matter on the Internet, the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communication; unauthorized access, including "hacking" and other unlawful activities by minors online; unauthorized disclosures, use, and dissemination of personal identification information regarding minors; and measures designed to restrict minors' access to materials harmful to minors.

The School district will certify, that all schools in the district, including media centers/libraries, are in compliance with the Children's Internet Protection Act. The school district will certify that the requirements of this policy are enforced. The district will post the Safe & Responsible Internet Use Plan on the district website, with links to this AUP, Regulation 2361, and recommended Internet safety sites for parents. An e-mail input mechanism requesting comments or concerns regarding the Safe & Responsible Internet Use Plan will be provided on the district web site.

Standards for Use

Any individual engaging in the following actions when using the district electronic network, computers and related resources shall be subject to discipline or legal action:

- Uses the network to publish any information that violates or infringes upon the rights of any other person or any
- information that would be abusive, profane or sexually offensive to an average person.
- Uses the network, computers or related resources to submit, publish or display any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive or otherwise illegal material; nor shall a user encourage the use, sale or distribution of controlled substances. *Illegal activities are defined as activities that violate federal, state, local laws and regulations. Obscene activities shall be defined as violation of generally accepted social standards for use of publicly owned and operated communication vehicles.*
- Transmission of material, information or software that is in violation of local, state or federal laws.
- Violate copyright, plagiarism, institutional or third party copyright, license agreements or other contracts.

- Uses the district network in a manner that intentionally disrupts network traffic or crashes the network; degrades or disrupts equipment or system performance;
- Uses the computing resources of the school district for commercial purposes, financial gain or fraud;
- Steals data or other intellectual property;
- Gains or seek unauthorized access to the files of others or vandalizes the data of another user;
- Gains or seeks unauthorized access to resources or entities;
- Forges electronic mail messages or uses an account owned by others;
- Invades privacy of others;
- Posts anonymous messages;
- Engages in other activities that do not advance the educational purposes for which the network, computers, and related resources are provided.
- Violates the online provisions outlined in Regulation 2361 which address E-mail usage, the Internet, Videoconferencing, Interactive Communication Areas, and Web Site creation.
- Violates the provisions outlined in Regulation 2361 that address supervision, monitoring, search and seizure and retention of records.
- Violates the provisions outline in Regulation 2361 that address safety and security of minors, and network security and vandalism.
- Violates provisions outlined in Regulation 2361 that address software, files, hardware, peripherals, other technology equipment and resources, and third party systems.

Consent Requirement

No student shall be allowed to use the district electronic network, computers and related resources unless they have filed with the principal an Acceptable Use Policy Consent Form agreement that is signed by the student and his/her parent(s) or guardian(s). A Student Acceptable Use Policy and Internet Safety Plan will be attached to the consent form for review by the parent/guardian.

Staff are not required to sign a consent and waiver agreement. Staff have an obligation to abide by district policies and

regulations as a part of their employment responsibilities. Failure to abide by district regulations and policies is handled through a disciplinary process in accord with district regulations, policies, and state and federal law.

No Guest user shall be allowed to use the district electronic network, computers and related resources unless they have filed with a district administrator an Acceptable Use Policy Consent Form agreement that is signed by the user and his/her parent(s) or guardian(s) if a minor. A Guest user Acceptable Use Policy and Internet Safety Plan will be attached to the consent form for review.

Violations of Regulation and Policy 2361

1. Violations of this Acceptable Use Policy and Regulation 2361 may result in a loss of access as well as other disciplinary or legal action.
2. Student disciplinary action shall be taken as indicated in Policy and Regulation numbers 2361, Acceptable use of District Electronic Network, Computers and Related Resources, No. 5600, Pupil Discipline, No. 5610, Suspension and No. 5260. Expulsion as well as possible legal action and reports to the legal authorities and entities could result. Students violating this policy shall be subject to the consequences as indicated in Regulation number 2361 and other appropriate discipline, which includes but is not limited to:
 - Use of district network only under direct supervision
 - Suspension of network privileges
 - Revocation of network privileges
 - Suspension of computer privileges
 - Revocation of computer privileges
 - Suspension from school
 - Expulsion from school and/or
 - Legal action and prosecution by the authorities.

The particular consequences for violations of this Policy shall be determined by the Superintendent in matters relating to the use of the network and by the principals in matters of school suspension. The superintendent or designate and the board shall determine when school expulsion and/or legal action or actions by the authorities are the appropriate course of action. Decisions

may be appealed in accordance with Policy number 5710 Pupil Grievances.

3. Staff and Guest users violating Regulation and Policy 2361 shall be subject to the discipline code outlined in the district policies and regulations regarding discipline as well as other disciplinary or possible legal action and reports to the legal authorities and entities.

Date Adopted: 9/17/96
Date Revised: 7/16/02
Second Revision: 10/7/02
Third Revision: 5/16/07