

Mechanicsburg Area School District
Acceptable Use Policy

**ACCEPTABLE USE OF THE COMPUTERS, NETWORK,
INTERNET, ELECTRONIC COMMUNICATIONS, AND INFORMATION POLICY**
(from MASD Policy #815, "Acceptable Use of Internet")

Purpose

The Mechanicsburg School District provides employees, students and guests ("users") with access to the District's electronic communication systems and network, which includes Internet access, whether wired or wireless, or by any other means.

Computers, network, Internet, electronic communications and information systems (collectively "CIS") provide vast, diverse and unique resources. The Board will provide access to the District's CIS for employees and for students in order to access information, research, to facilitate learning and teaching, and to foster the educational purpose and mission of the Mechanicsburg School District.

For users, the District's CIS must be used primarily for education-related purposes and performance of professional job duties. *Incidental personal use* of school computers is permitted for employees so long as such use does not interfere with the employee's job duties and performance, with system operations, or with other system users. Personal use must comply with this policy and all other applicable Mechanicsburg School District policies, procedures and rules contained in this policy, local, state and federal laws. Students may only use the CIS systems for educational purposes. At the same time, employees' and students' personal technology devices brought onto the District's property or suspected to contain District information may be legally accessed to insure compliance with this Policy and other District policies to protect the District's resources, and to comply with the law. Users may not use their personal computers to access the School District's intranet, Internet or any other CIS unless approved by the Technology Coordinator and/or designee.

The Mechanicsburg School District intends to strictly protect its CIS against numerous outside and internal risks and vulnerabilities. Users are important and critical players in protecting these District assets and in lessening the risks that can destroy these important and critical assets. Consequently, guests, employees and students are required to fully comply with this policy, and to immediately report any violations or suspicious activities to the Technology Coordinator.

Authority

1. Access to the Mechanicsburg School District CIS systems through school resources is a privilege, not a right. These, as well as the user accounts and information, are the property of the Mechanicsburg School District, which reserves the right to deny access to prevent further unauthorized, inappropriate or illegal activity, and may revoke those privileges and/or administer appropriate disciplinary action. The District will cooperate to the extent legally required with the ISP, local, state and federal officials in any investigation concerning or related to the misuse of the CIS systems.

2. It is often necessary to access user accounts in order to perform routine maintenance and security tasks; system administrators have the right to access by interception, and the stored communication of user accounts for any reason in order to uphold this policy and to maintain the system. Users have no privacy expectation in the contents of their personal files or any of their use of the District's CIS. The District reserves the right to monitor, track, log and access CIS use and to monitor and allocate filespace.

3. The District reserves the right to restrict access to any Internet sites or functions it may deem inappropriate through software blocking or general policy. Specifically, the District operates and enforces technology protection measure(s) that block or filter online activities of minors on its computers used and accessible to adults and students so as to filter or block inappropriate matter on the Internet. Inappropriate matter includes, but is not limited to, visual, graphic, text and any other form of obscene, sexually explicit, child pornographic, or other material that is harmful to minors, hateful, illegal, defamatory, lewd, vulgar, profane, rude, inflammatory, threatening, harassing, discriminatory (as it pertains to race, color, religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid, or disability), violent, bullying, terroristic, and advocates the destruction of property. Measures designed to restrict adults' and minors' access to material harmful to minors may be disabled to enable an adult to access bona fide research or for another lawful purpose.

Mechanicsburg Area School District
Acceptable Use Policy

4. The District has the right, but not the duty, to monitor, track, log, access and report all aspects of its computer information technology and related systems of all users and of any employee's, student's and guest's personal computers, network, Internet, electronic communication systems, and media brought on to District premises or at District events, connected to the District network, containing District programs or District or student data (including images, files, and other information) to insure compliance with this policy and other District policies, to protect the District's resources, and to comply with the law.

5. The District reserves the right to restrict or limit usage of lower priority CIS systems and computer uses when network and computing requirements exceed available capacity according to the following priorities:

- a. Highest – uses that directly supports the education of the students.
- b. Medium – uses that indirectly benefit the education of the student.
- c. Lowest – uses that include reasonable and limited educationally-related interpersonal communications and incidental personnel communications.
- d. Forbidden – all activities in violation of this policy.

6. The District additionally reserves the right to:

- a. Determine which CIS services will be provided through District resources.
- b. View and monitor network traffic, file server space, processor, and system utilization, and all applications provided through the network and communications systems, including e-mail.
- c. Remove excess e-mail or files taking up an inordinate amount of fileserver disk space after a reasonable time.
- d. Revoke user privileges, remove user accounts, or refer to legal authorities when violation of this and any other applicable District policies occur or state or federal law is violated, including, but not limited to, those governing network use, copyright, security, privacy, employment, and destruction of District resources and equipment.

Responsibility

1. Due to the nature of the Internet as a global network connecting thousands of computers around the world, inappropriate materials, including those which may be defamatory, discriminatory (as it pertains to race, color, religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid, or disability), inaccurate, obscene, sexually explicit, lewd, vulgar, rude, harassing, violent, inflammatory, threatening, terroristic, hateful, bullying, profane, pornographic, offensive, and illegal, can be accessed through the network and electronic communications systems. Because of the nature of the technology that allows the Internet to operate, the District cannot completely block access to these resources. Accessing these and similar types of resources may be considered an unacceptable use of school resources and will result in disciplinary actions.

2. Users must become proficient in the use of the District's CIS, and software relevant to the employee's responsibilities and practice proper etiquette, ethical behavior, and agree to the requirements of this policy.

a. Etiquette users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to the following:

- (1) Be polite. Do not become abrasive in messages to others. General District rules and policies for behavior and communicating apply.
- (2) Use appropriate language. Do not swear or use vulgarities or other inappropriate language.
- (3) Do not reveal the personal addresses or telephone numbers of others.
- (4) Recognize that e-mail is not private or confidential.
- (5) Do not use the Internet or e-mail in any way that would interfere with or disrupt its use by other users.
- (6) Consider all communications and information accessible via the Internet to be the property of the District.
- (7) Do not order any materials or use credit cards while using the District's computers.
- (8) Respect the rights of other users to an open and hospitable technology environment, regardless of race, sexual orientation, color, religion, creed, ethnicity, age, marital status or handicap status.

Mechanicsburg Area School District
Acceptable Use Policy

Delegation of Responsibility

1. The Technology Coordinator and/or designee will serve as the coordinator to oversee the District's CIS and will work with other regional or state organizations as necessary, to educate employees, approve activities, provide leadership for proper training for all users in the use of the CIS and the requirements of this policy, establish a system to insure adequate supervision of the CIS, maintain executed user agreements, and interpret and enforce this policy.

2. The Technology Coordinator and/or designee will establish a process for setting-up individual and class accounts, set quotas for disk usage on the system, establish a retention schedule, and establish the District's virus protection process.

3. Unless otherwise denied for cause, student access to the CIS resources shall be through supervision by the professional staff. Administrators, teachers and staff have the responsibility to work together to help students develop the skills and judgment required to make effective and appropriate use of the resources. All users have the responsibility to respect the rights of all other users within the District and school district CIS, and to abide by the rules established by the District.

Guidelines

1. Access to the CIS

- a. CIS user accounts will be used only by authorized owners of the accounts for authorized purposes.
- b. An account will be made available according to a procedure developed by appropriate District authorities.
- c. CIS. The District's Acceptable Use of the Computers, Network, Internet, Electronic Communications, and Information Policy, as well as other relevant District policies, will govern use of the District's CIS systems for students, employees and guests. Use of the CIS will also be governed by the other relevant District policies, and where applicable, school district policies in which the CIS systems are located.
- d. Types of Services included, but not limited to:
 - (1) World Wide Web. District employees, students, and guests will have access to the Web through the District's CIS as needed.
 - (2) E-Mail. District employees and may be provided assigned individual e-mail accounts for work related, and incidental personal use, as needed.
 - (3) Guest Accounts. Guests, which include but are not limited to, visitors, workshop attendees, volunteers, independent contractors and adult education instructors, may receive an individual Internet account with the approval of the Technology Coordinator and/or designee if there is a specific, District-related purpose requiring such access. Use of the computers, network, and Internet by a guest must be specifically limited to District related purpose. An agreement will be required and parental signature will be required if the guest is a minor and given unsupervised access.
- e. Access to all data on, taken from, or compiled using District computers is subject to inspection and discipline. Users have no right to expect that District information placed on users' personal computers, networks, Internet, and electronic communications systems is beyond the access of the District. The District reserves the right to legally access users' personal equipment for District information.

2. Parental Notification and Responsibility

The District will notify the parents about the District's CIS systems and the policies governing their use. This policy contains restrictions on accessing inappropriate material. There is a wide range of material available on the Internet, some of which may not be fitting with the particular values of the families of the students. It is not practically possible for the District to monitor and enforce a wide range of social values in student use of the Internet. Further, the District recognizes that parents bear primary responsibility for transmitting their particular set of family values to their children. The District will encourage parents to specify to their child(ren) what material is and is not acceptable for their child(ren) to access through the District's CIS system. Teachers are responsible for their students' use of the District's CIS systems when the students are under their supervision.

Mechanicsburg Area School District
Acceptable Use Policy

3. District Limitation of Liability

The District makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the District's CIS systems will be error-free or without defect. The District does not warrant the effectiveness of Internet filtering. The electronic information available to users does not imply endorsement of the content by the District, nor is the District responsible for the accuracy or quality of the information obtained through or stored on the CIS systems. The District shall not be responsible for any damage users may suffer, including but not limited to, information that may be lost, damaged, delayed, misdelivered, or

Acceptable Use Policy (cont'd.)

unavailable when using the computers, network and electronic communications systems. The School District will not be responsible for stolen, damaged, or lost personal devices of students, employees, contractors and guests. The District shall not be responsible for material that is retrieved through the Internet, or the consequences that may result from them. The District shall not be responsible for any unauthorized financial obligations, charges or fees resulting from access to the District's CIS systems. In no event shall the District be liable to the user for any damages whether direct, indirect, special or consequential, arising out the use of the CIS systems.

4. Prohibitions

The use of the District's CIS for illegal, inappropriate, unacceptable, or unethical purposes by users is prohibited. Such activities engaged in by users are strictly prohibited and illustrated below. The District reserves the right to determine if any activity not appearing in the list below constitutes an acceptable or unacceptable use of the CIS.

These prohibitions are in effect any time District resources are accessed whether on District property, when using mobile commuting equipment, telecommunication facilities in unprotected areas or environments, directly from home, or indirectly through another ISP, and if relevant, when an employee, student or guest uses their own equipment.

Students are prohibited from visibly possessing and using their personal computers, as defined in this policy, on District premises and property (including but not limited to, buses and other vehicles), at District events, or through connection to the District's CIS, unless expressed permission has been granted by the technology coordinator or designee, who will then assume the responsibility to supervise the student in its use, or, unless an IEP team determines otherwise, in which case, an employee will supervise the student in its use. Students who are performing volunteer fire company, ambulance or rescue squad functions, or need such a computer due to their medical condition, or the medical condition of a member of their family, with notice and the approval of the school administrator may qualify for an exemption of this prohibition.

a. General Prohibitions

Users are prohibited from using District CIS to:

- (1) Communicate about non-work or non-school related communications unless the employees' use comports with this policy's definition of incidental personal use.
- (2) Access or transmit material that is harmful to minors, indecent, obscene, pornographic, child pornographic, terroristic, or advocates the destruction of property.
- (3) Access or transmit material likely to be offensive or objectionable to recipients including, but not limited to, that which may be defamatory, inaccurate, obscene, sexually explicit, lewd, hateful, harassing, discriminatory (as it pertains to race, color, religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid, or disability), violent, vulgar, rude, inflammatory, threatening, profane, pornographic, offensive, terroristic and/or illegal.
- (4) Cyberbullying another individual.
- (5) Access or transmit gambling, pools for money, including but not limited to, basketball and football, or any other betting or games of chance.
- (6) Participate in discussion or news groups that cover inappropriate and/or objectionable topics or materials, including those that conform to the definition of inappropriate matter in this policy.
- (7) Send terroristic threats, hateful mail, harassing communications, discriminatory

**Mechanicsburg Area School District
Acceptable Use Policy**

remarks, and offensive or inflammatory communications.

- (8) Participate in unauthorized Internet Relay Chats, instant messaging communications and Internet voice communications (on-line; real-time conversations) that are not for school-related purposes or required for employees to perform their job duties.
- (9) Facilitate any illegal activity.
- (10) Communicate through e-mail for non-educational purposes or activities, unless it is for an incidental personal use as defined in this policy. The use of e-mail to mass mail non-educational or no-work related information is expressly prohibited.
- (11) Engage in commercial, for-profit, or any business purposes (except where such activities are otherwise permitted or authorized under applicable District policies); conduct unauthorized fund raising or advertising on behalf of the District and non-school District organizations; resell of District computer resources to individuals or organizations, who are not related to the District; or use the District's name in any unauthorized manner that would reflect negatively on the District, its employees, or students. Commercial purposes are defined as offering or providing goods or services or purchasing goods or services for personal use. District acquisition policies will be followed for District purchase of goods or supplies through the District system.
- (12) Political lobbying.
- (13) Install, distribute, reproduce or use copyrighted software on District computers, or copy District software to unauthorized computer systems, intentionally infringing upon the intellectual property rights of others or violating a copyright.
- (14) Install computer hardware, peripheral devices, network hardware or system hardware. The authority to install hardware or devices on District computers is restricted to the Technology Coordinator or designee.
- (15) Encrypt messages using encryption software that is not authorized by the District from any access point on District equipment or District property. Employees and students must use District approved encryption to protect the confidentiality of sensitive or critical information in the District's approved manner.
- (16) Access, interfere, possess, or distribute confidential or private information without permission of the School District administration. An example includes accessing other students' accounts to obtain their grades.
- (17) Violate the privacy or security of electronic information.
- (18) Use the systems to send any District information to another party, except in the ordinary course of business as necessary or appropriate for the advancement of the District's business, or educational interest.
- (19) Sending unsolicited commercial electronic mail messages, also known as spam.
- (20) Posting personal or professional web pages that are not part of the approved District web page solution.
- (21) Posting anonymous messages.

b. Access and Security Prohibitions

Users must immediately notify the Technology Coordinator and/or designee if they have identified a possible security problem. Students, employees, and guests must read, understand, provide signed acknowledgment form and comply with this policy that includes network, Internet usage, electronic communications, telecommunications, non-disclosure and physical information security policies. The following activities related to access to the District's CIS, and are prohibited.

- (1) Misrepresentation (including forgery) of the identity of a sender or source of communication.
- (2) Acquiring or attempting to acquire passwords of others or giving your password to another. Users will be held responsible for the result of any misuse of the users' user name or password while the users' systems access were left unattended and accessible to others, whether intentional or through negligence.
- (3) Using or attempting to use computer accounts of others, these actions are illegal.
- (4) Altering a communication originally received from another person or computer with

Mechanicsburg Area School District
Acceptable Use Policy

the intent to deceive.

- (5) Using District resources to engage in any illegal act, which may threaten the health, safety or welfare of any person or persons, such as arranging for the promotion of or the sale of drugs, alcohol, or weapons, engaging in criminal activity, or being involved in a terroristic threat against any person or property.
- (6) Disabling or circumventing any District security, program or device, for example, but not limited to, anti-spyware, anti-spam software, and virus protection software or procedures.
- (7) Transmitting electronic communications anonymously or under an alias unless authorized by the Intermediate Unit.

c. Operational Prohibitions

The following operational activities and behaviors are prohibited.

- (1) Interference with or disruption of the CIS systems, network accounts, services or equipment of others, including, but not limited to, the propagation of computer “worms” and “viruses”, Trojan Horse and trapdoor program code, the sending of electronic chain mail, distasteful jokes, and the inappropriate sending of “broadcast” messages to large numbers of individuals or hosts. The user may not hack or crack the network or others’ computers, whether by parasiteware or spyware designed to steal information, or viruses and worms or other hardware or software designed to damage the CIS, or any component of the network, or strip or harvest information, or completely take over a person’s computer, or to “looking around”.
- (2) Altering or attempting to alter files, system security software or the systems without authorization.
- (3) Unauthorized scanning of the CIS systems for security vulnerabilities.
- (4) Attempting to alter any District computing or networking components (including, but not limited to file servers, bridges, routers, or hubs) without authorization or beyond one’s level of authorization.
- (5) Unauthorized wiring, including attempts to create unauthorized network connections, or any unauthorized extension or re-transmission of any computer, electronic communications systems, or network services, whether wired, wireless, cable, or by other means.
- (6) Connecting unauthorized hardware and devices to the CIS such as PDAs, portable gaming systems, computers. USB storage drives (also known as pen drives, flash drives, key drives, jump drives), or any other personal storage device (CD-R; DVD-R) will be permitted for school related file transfers.
- (7) Loading, downloading, or use of unauthorized games, programs, files, or other electronic media, including, but is not limited to, downloading music files.
- (8) Intentionally damaging or destroying the integrity of the District’s electronic information.
- (9) Intentionally destroying the District’s computer hardware or software.
- (10) Intentionally disrupting the use of the CIS.
- (11) Damaging the District’s CIS, networking equipment through the users’ negligence or deliberate act.
- (12) Failing to comply with requests from appropriate teachers or District administrators to discontinue activities that threaten the operation or integrity of the CIS.
- (13) Use of audio or video recording devices without first obtaining consent of subject/person to be recorded.

5. Content Guidelines

Information electronically published on the District’s CIS shall be subject to the following guidelines:

- a. Published documents including but not limited to audio and video clips or conferences, may not include a child’s picture, phone number, street address, or box number, name (other than first name) or the names of other family members without parent consent.
- b. Documents, web pages, electronic communications, or videoconferences may not include personally identifiable information that indicates the physical location of a student at a given

Mechanicsburg Area School District
Acceptable Use Policy

time without parent consent.

Acceptable Use Policy (cont'd.)

- c. Documents, web pages, electronic communications, or videoconferences may not contain objectionable materials or point directly or indirectly to objectionable materials.
- d. Documents, web pages and electronic communications, must conform to all District policies and guidelines, including the copyright policy.
- e. Documents to be published on the Internet must be edited and approved according to District procedures before publication.

6. Due Process

- a. The District will cooperate with the Intermediate Unit, local, state, and federal officials to the extent legally required in investigations concerning or relating to any illegal activities conducted through the District's CIS.
- b. If students or employees possess due process rights for discipline resulting from the violation of this policy, they will be provided such rights.
- c. The District may terminate the account privileges by providing notice to the user

7. Search and Seizure

- a. Users' violations of this Policy, any other District policy, or the law may be discovered by routine maintenance and monitoring of the District Network system, or any method stated in this policy, or pursuant to any legal means.
- b. The District reserves the right to monitor, track, log and access any electronic communications, including but not limited to, Internet access and e-mails at any time for any reason. Users should not have the expectation of privacy in their use of the District's CIS, and other District technology, even when used for personal reasons. Further, the District reserves the right, but not the obligation, to access any personal technology device of users brought onto the District premises or at District events, or connected to the District network, containing District programs or District or student data (including images, files, and other information) to insure compliance with this policy and other District policies, to protect the District resources, and to comply with the law.
- c. Everything that users place in their personal files should be written as if a third party will review it.

8. Copyright Infringement and Plagiarism

- a. Federal laws, cases, and guidelines pertaining to copyright will govern the use of material accessed through the District resources. Users will make a standard practice of requesting permission from the holder of the work and complying with license agreements. Employees will instruct students to respect copyright, request permission when appropriate, and comply with license agreements and employees will respect and comply as well.
- b. Violations of copyright law can be a felony and the law allows a court to hold individuals personally responsible for infringing the law. The District does not permit illegal acts pertaining to the copyright law. Therefore, any user violating the copyright law does so at their own risk and assumes all liability.
- c. Violations of copyright law include, but are not limited to, the making of unauthorized copies of any copyrighted material (such as commercial software, text, graphic images, audio and video recording), distributing copyrighted materials over computer networks, and deep-linking and framing into the content of others' web sites. Further, the illegal installation of copyrighted software or files for use on the District computers is expressly prohibited. This includes all forms of licensed software – shrink-wrap, clickwrap, browsewrap, and electronic software downloaded from the Internet.
- d. District guidelines on copyright and plagiarism will govern use of material accessed through the District's CIS. Users will not plagiarize works that they find. Teachers will instruct students in appropriate research and citation practices.

Mechanicsburg Area School District
Acceptable Use Policy

Acceptable Use Policy (cont'd.)

9. Selection of Material

- a. Board policies on the selection of materials will govern use of the District's CIS.
- b. When using the Internet for class activities, teachers will select material that is appropriate in light of the age of the students and that is relevant to the course objectives. Teachers will preview the materials and web sites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the web site. Teachers will provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers will assist their students in developing the critical thinking skills necessary to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.

10. District Web Site

- a. The District will establish and maintain a Web Site and will develop and modify its Web pages that will present information about the District under the direction of the Technology Coordinator and/or designee. Web Site creation and content must be approved through the Technology Coordinator or designee.

11. Safety & Privacy

- a. To the extent legally required, users of the District's CIS systems will be protected from harassment or commercially unsolicited electronic communication. Any user who receives threatening or unwelcome communications must immediately take them to the Technology Coordinator and/or designee.
- b. Users will not post personal contact information about themselves or other people on the CIS. The user may not steal another's identity in any way, may not use spyware, parasiteware, cookies, or use District or personnel employee technology or resources in any way to invade one's privacy. Additionally, the user may not disclose, use or disseminate confidential and personal information about students or employees.
- c. Student users will agree not to meet with someone they have met online unless they have parent consent.

12. Consequences for Inappropriate, Unauthorized and Illegal Use

- a. General rules for behavior, ethics, and communications apply when using the CIS and information, in addition to the stipulations of this policy. Users must be aware that violations of this policy or other policies, or for unlawful use of the CIS may result in loss of CIS access and a variety of other disciplinary actions, including but not limited to, warnings, usage restrictions, loss of privileges, position reassignment, oral or written reprimands, suspensions, dismissal, expulsions, and/or legal proceedings on a case-by-case basis. This policy incorporates all other relevant District policies.
- b. The user is responsible for damages to the network, equipment, electronic communications systems, and software resulting from deliberate and willful acts. The user will also be responsible for incidental or unintended damage resulting from willful or deliberate violations of this policy.
- c. Violations as described in this policy may be reported to the Technology Coordinator. The District will cooperate to the extent legally required with authorities in all such investigations.
- d. Vandalism will result in cancellation of access to the District's, CIS and resources and is subject to disciplinary action.

Mechanicsburg Area School District
Acceptable Use Policy

Acceptable Use Policy (cont'd.)

APPENDIX 1 –Definitions of Terms used in Policy

1. Access to the Internet – A computer shall be considered to have access to the Internet if the computer is equipped with a modem or is connected to a network that has access to the Internet, whether by wire, wireless, cable, or any other means.

2. Child Pornography – Any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

3. Computer – Includes any District owned, leased or licensed or employee, student and guest owned personal hardware, software, or other technology used on District premises or at District events, or connected to the District network, containing District programs or District or student data (including images, files, and other information) attached or connected to, installed in, or otherwise used in connection with a computer. Computer includes, but is not limited to, District, employee, students and guest: desktop, notebook, tablet PC or laptop computers, printers, cables, modems, and other peripherals; specialized electronic equipment used for students' special educational purposes; global position system (GPS) equipment; personal digital assistants (PDAs); cell phones, with or without Internet access and/or recording and/or camera and other capabilities, mobile phones, or wireless devices; two-way radios/telephones; portable gaming devices; laser pointers, and any other such technology developed.

4. Electronic Communications Systems – Any messaging, collaboration, publishing, broadcast, or distribution system that depends on electronic communications resources to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across electronic communications network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic communications or is implicitly used for such purposes. Further, an electronic communications system means any wire, radio, electromagnetic, photo optical or photo electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. Examples include, but are not limited to, the Internet, intranet, electronic mail services, Global Positioning Systems, Personal Digital Assistants, cell phones with or without Internet access and/or electronic mail and/or recording devices, cameras, and other capabilities.

5. Educational Purpose – Includes use of the CIS for classroom for classroom activities, professional or career development, and to support the District's curriculum, policy and mission statement.

6. Harmful to Minors – Any picture, image, graphic image file or other visual depictions that taken as a whole, with respect to minors, appeals to the prurient interest in nudity, sex, or excretion; depicts, describes, or represents in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual content, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals, and taken as a whole lacks serious literary, artistic, political, or scientific value as to minors.

7. Incidental Personal Use – Use of District CIS by an individual employee for occasional personal communications. Personal use must comply with this policy and all other District policies, procedures and rules, as well as ISP, local, state and federal laws and may not interfere with the employee's job duties and performance, with system operations, or with other system users, and must not damage the District's CIS systems. Under no circumstances should the employee believe their use is private. The District reserves the right to monitor, track, access, and log the use of its CIS systems at any time.

Mechanicsburg Area School District
Acceptable Use Policy

8. Minor – For purposes of compliance with the Children’s Internet Protection Act (“CIPA”), an individual who has not yet attained the age of seventeen. For other purposes, minor shall mean the age of minority as defined in the relevant law.

Acceptable Use Policy (cont’d.)

9. Network – A system that links two or more computer systems, including all components necessary to effect the operation, including, but not limited to: computers, copper and fiber cabling, wireless communications and links, equipment closets and enclosures, network electronics, telephone lines, printers and other peripherals, storage media, software, and other computers and/or networks to which the District network may be connected, such as the Internet, the Internet2, or those of other institutions.

10. Obscene – Analysis of the material meets the following elements. Whether the average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest; whether the work depicts or describes, in a patently offensive way, sexual conduct specifically designed by the applicable state or federal law to be obscene; and whether the work taken as a whole lacks serious literary, artistic, political, or scientific value.

11. Technology Protection Measure(s) – A specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors.

12. Visual Depictions – Undeveloped film and videotape and data stored on computer disk or by electronic means which is capable of conversion into a visual image but does not include mere words.