

MIDDLETOWN AREA SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE FOR TECHNOLOGY

ADOPTED: March 16, 1998

REVISED: August 22, 2011

<p>1. Purpose</p> <p>1. Definition</p> <p>3. Authority</p> <p>20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254</p>	<p style="text-align: center;">815. ACCEPTABLE AND SAFE USE FOR TECHNOLOGY</p> <p>Middletown Area School District (MASD) requires the appropriate use of technology as part of our instructional program.</p> <p>For purposes of this policy, the term Technology includes, but is not limited to, Internet access, computers, tablets, electronic devices, email, and desktop and online applications.</p> <p>This policy pertains to all technology used in the district, including district purchased technology devices and personal purchased technology devices. All personal purchased technology devices used inside the district may be accessed when a reasonable belief exists that such usage does not comply with this policy and other district policies or is necessary to protect district resources or comply with the law.</p> <p>All technology must be primarily used for educational purposes and performance of job duties. Personal use of district purchased technology is permitted for employees only, as long as such use does not interfere with the employee’s job duties. Incidental personal use of district purchased technology is permitted for employees only, as long as such use does not: (1) interfere with the employee’s job duties or performance, with system operations, or with other system users; (2) undermine the District’s educational mission or adversely impact the District’s reputation; and (3) complies fully with the terms of all District policies. Personal use of technology may only occur during non-work time, such as before and after an employee’s scheduled work day or during a scheduled break. Personal use of technology is prohibited by any employee during any time when in the presence of a student. Any such personal use must comply with all local, state, and federal policies, rules, and regulations and must not damage or harm any users or other technology. The district reserves the right to terminate an employee’s privilege to use district technology for personal use for any reason at any time.</p> <p>Information accessed inside the district, via technology, does not imply endorsement by the district. The district, through best effort systems, will filter and/or monitor information accessed via the Internet, but does not guarantee that all content considered inappropriate will be blocked by such systems. The district shall not be</p>
--	--

<p>4. Delegation of Responsibility</p>	<p>responsible for any information that may be lost, damaged, or unavailable when using the network or for any information that is retrieved via the Internet.</p> <p>The district reserves the right to monitor and log all use of technology inside the district, while making all attempts to respect the privacy rights of all users. Monitoring may include, but not be limited to, viewing files, emails, and Internet use for any user inside the district.</p> <p>District employees will be given local administrator rights on district computers so that they may install legally acquired software and software updates that will be used for educational or district business purposes. District employees are expected to abide by all software license agreements and copyright laws. District employees who install software do so at their own risk and in the event that a computer becomes non-functioning agree that the computer will be restored back to its original computer image by a member of the district's technology staff.</p> <p>All users are expected to use technology in a safe, appropriate manor and when in violation of this policy may have their privileges revoked. This Acceptable Use Policy for Technology establishes guidelines for such use.</p> <p>The district will take reasonable measures to ensure that all uses of technology by all users are done in a responsible and respectful manner.</p> <p>All users are expected to respect and protect the rights of other users, both inside and outside the district. The district expects all employees to uphold this policy and to provide guidance and instruction to students in the appropriate use of technology. Any employee who observes any use of technology in violation of this policy or seen as inappropriate by any user is expected to report such activities immediately to the proper authorities.</p>
<p>5. Guidelines</p>	<p>Appropriate or inappropriate use of technology shall be determined by the district's administrative team.</p> <p>All users, excluding guests, will be given a network account for purposes of gaining access to network resources, network storage, and the Internet. All district employees and student in grades 3 - 12 will be provided with an email account for its authorized purpose. All communications and information created with or on district technology should be assumed to be the property of Middletown Area School District. The disclosure of any student and/or employee information or other electronic files shall only be done by authorized personnel and in conformance with existing district policies and applicable state and federal laws and guidelines</p> <p>Any communications done via technology with parents/guardians, teachers, and other MASD staff regarding students may become part of the student's permanent record. Therefore, the district expects staff to communicate with student's</p>

parents/guardians in a professional and appropriate manner. All staff email will be archived according to the districts email archiving procedure for one (1) year from its send or receipt date. Thereafter, the district shall purge its email archives in conformance with those procedures to ensure adequate electronic storage on its server. The District reserves the right to archive or otherwise retain e-mails beyond this one (1) year retention period in order to comply with a litigation hold placed as a result of contemplated or actual litigation involving the School District, or when the retention of such e-mails is deemed appropriate by the District

Prohibitions

All users are expected to use technology in a safe, appropriate and legal manner in accordance with district policy. With respect to all users, the following uses are prohibited:

1. Use for or in inappropriate or illegal purposes or activities.
2. Use to access, view or obtain material that is inappropriate for minors, sexually explicit or pornographic in nature.
3. Use of another person's email address or user account
4. Use to access, copy, or modify email, files, passwords, data or information belonging to other users or deliberately interfering with the ability of other user's use of technology.
5. Use to misrepresent other users on the network.
6. The illegal or unauthorized installation, distribution, reproduction, or use of copyrighted or inappropriate software.
7. Use which constitutes a copyright violation or copying, downloading or distributing copyrighted material without the owner's permission, unless it is permitted in accordance with the fair use guidelines.
8. The unauthorized access, disclosure, use, or dissemination of personal information involving a student, employee or taxpayer.
9. Posting anonymous messages using district technology.
10. Use for purposes of accessing, sending, creating or posting materials, or communications that are defamatory, obscene, sexually explicit, threatening, harassing, promoting illegal activities or contrary to the school district policies, including the policy prohibitions against harassment and unlawful discrimination.

11. Use to upload, create, or distribute a computer virus or attempts to do the same.
12. Use to disrupt the work of other persons (the hardware or software of other persons shall not be destroyed, modified, or abused in any way).
13. Use for commercial, private advertisement, or 'for-profit' purposes.
14. Use for lobbying or political purposes.
15. Use to infiltrate or interfere with a computer system and/or damage the data, files, operations, software, or hardware components of a computer or system.
16. Use while access privileges are suspended or revoked.
17. Any attempt to circumvent or disable the Internet filter or any security measure installed by the district.
18. Use inconsistent with network etiquette and other generally accepted etiquette.
19. Use to post the photograph, work, or information of any student without a signed media release form on file.
20. Engaging in or accessing chat rooms, instant messaging, text messaging or file sharing for non-educational/non-work related purposes.
21. Sending or forwarding spam emails.

In addition to the prohibitions outlined above, users shall not use district technology resources to engage in gambling, commercial activities, partisan political activities or communications that would impair the reputation of the district.

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. Avoid being abusive in messages to others. Comply with general district and building rules and policies for behavior and communication.
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 email, instant messaging, and/or text messaging is not private or

confidential.

5. Respect the rights of other users to an open and hospitable technology environment.
6. Refrain from creating, distributing or condoning any message that disparages another individual because of his/her race, sexual orientation, color, religion, creed, ethnicity, age, marital status, or handicap status

Security

Security, as it pertains to technology, is protected through the use of passwords. All users are expected to protect their passwords and update/change them as indicated in the districts technology security procedures or when a password is thought to have been breached. To protect all technology systems, the following guidelines should be followed:

1. Users should not share or distribute their password to other users.
2. Use technology that is logged in under another user's credentials.
3. Users should understand that all use of technology is subject to monitoring, logging, and archiving in accordance with local, state, and federal rules and regulations.

Data Confidentiality

All personally identifiable student and employee information shall be treated as strictly confidential and shall not be disclosed to a third party without a legitimate educational or workplace purpose. Employee shall check with their immediate supervisors, if they have any question whether they are authorized to share an individual's personally identifiable information. In addition, access to such data shall be allowed only if necessary in the performance of that persons work responsibilities. All other access must be authorized in writing by the assigned data custodian. In addition:

1. No aggregate data from such records shall be reported or published without written permission of the data custodian.
2. Data may not be copied or stored in any format outside of approved backup procedures.
3. Developers may not copy data for development and testing purposes without the written permission of the data custodian.

4. Access to production, acceptance test, and development data, shall be protected in accordance with the requirements of the data custodian.
5. Any breach, or suspected breach, of data confidentiality shall be reported immediately to the Superintendent.

A violation of the data confidentiality provisions by a user may result in the imposition of discipline, which may include termination from employment or expulsion from school. The district reserves the right to report the improper accessing or disclosure of confidential data to law enforcement officials for criminal prosecution.

PROCEDURES

Monitoring –

The district reserves the right to log, monitor, and review Internet, email, and other network use of all account holders. This logging, monitoring, and review may be conducted without cause and without notice. Each user (account holder) agrees and consents to such logging, monitoring, and review and acknowledges that he/she has no right or expectation of confidentiality or privacy with respect to Internet, email, or other network usage. The Director of Technology and the IT Systems Manager may review student and staff files and communications to maintain system integrity and ensure that the system is being utilized for appropriate purposes. Users should expect that files stored on district servers or computers will not be private.

Filter –

The district will employ the use of an Internet filter as a technology protection measure pursuant to the state and federal Children’s Internet Protection Act. This filter may be temporarily disabled by the Network Administrator at the workstation level for use by an adult administrator or teacher for bona fide research or other lawful purposes, so long as the workstation is not used by students and the filter disabling is authorized by the Superintendent. The filter may not be disabled for use by students or other minors for any reason.

Access Agreement –

All non-student users who intend to use district technology must agree to and abide by all conditions of this policy. Each non-student user wishing to use district technology must sign the Acceptable Use Policy Agreement prior to gaining access to any district technology. Non-student users refusing to sign the Acceptable Use Policy Agreement will not be given access to district technology.

INTERNET SAFETY

47 U.S.C.
Sec. 254

The School District will develop and maintain effective Internet Safety practices which aim to maximize the benefits of the Internet and technology devices/equipment to student learning and to the effective operation of the school, while minimizing and managing any risks. Internet Safety education will include topics such as cyberbullying awareness and response and interacting with other individuals on social networking sites and in chat rooms.

These Internet Safety practices will aim to address the needs of students and other members of the school community to receive education about the safe and responsible use of present and developing information and communication technologies.

To ensure proper Internet Safety practices, the School District will follow this set of guidelines:

1. No non-student user may use the School District's owned or leased technology in any circumstances unless the Acceptable and Safe Use Agreement has been signed and returned to the school. Use agreements also apply to the use of privately-owned/leased technology on the school site, or at/for any school-related activity, regardless of its location. This includes off-site access to the school network from school or privately-owned/leased equipment.
2. School District use agreements will cover all employees, all students (including adult and community), and any other individuals authorized to make use of the School District technology, such as student teachers, contractors, and other special visitors to the school.
3. The use agreements are also an educative tool and should be used as a resource for the professional development of staff.
4. Teachers and other professional staff will consistently remind students of Internet Safety practices through both formal and informal practices. Although the School District may offer formal Internet Safety education, it is expected that all staff will play a role in the continuous Internet Safety education of the School District's students.
5. Signed use agreements will be filed in a secure place, and an appropriate system devised which facilitates confirmation that particular individuals are authorized to make use of the Internet and ICT devices/equipment.
6. The safety of children is of paramount concern. Any apparent breach of Internet Safety will be taken seriously. In serious incidents, advice will be sought from an appropriate source, such as the School Solicitor or other legal professional with specialist knowledge in this area. There will be special

attention paid to the need for specific procedures regarding the gathering of evidence in potentially serious cases. If illegal material or activities are suspected, the matter may need to be reported to the relevant law enforcement agency.

CONSEQUENCES OF INAPPROPRIATE USE

Users shall be responsible for damages to technology resulting from their own reckless, deliberate or willful acts. Failure by any user to follow the procedures and prohibitions defined in this AUP may result in the temporary or permanent loss of access privileges to all or some district technology, as well as the imposition of other forms of discipline. Additionally, illegal activities or use (i.e., intentional deletion or damage to files or data belonging to others; copyright violations; etc.) may be reported to the appropriate legal authorities for possible prosecution. The district reserves the right to remove a user account from the network to prevent unauthorized, inappropriate, illegal activity or as a disciplinary measure against a user.

The use of technology resources is a privilege, not a right. The Superintendent, along with the Administrative team, shall be responsible for enforcing the requirements of this policy, including the assessment whether a user engaged in inappropriate use of district technology.

School District Limitation of Liability

The School District makes no warranties of any kind, whether express or implied, for the service it is providing. The School District is not responsible, and will not be responsible, for any damages, including loss of data resulting from delays, non-deliveries, missed deliveries, or service disruptions. Use of any information obtained through the use of the School District's computers is at the user's risk. The District assumes no responsibility for the quality or accuracy of information obtained through the Internet or emails.

The School District assumes no responsibility or liability for any charges incurred by a user under normal operating procedures.

References:

State Board of Education Regulations – 22 PA Code Sec. 403.1

Child Internet Protection Act – 24 P.S. Sec. 4601 et seq.

U.S. Copyright Law – 17 U.S.C. Sec. 101 et seq.

Enhancing Education Through Technology Act of 2001 – 20 U.S.C. Sec. 6777

	<p>Internet Safety – 47 U.S.C. Sec. 254</p> <p>Board Policy – 814</p>
--	---